

DIGITAL TELEVISION METHODS AND APPARATUS

Publication number: JP2003515286 (T)

Publication date: 2003-04-22

Inventor(s):

Applicant(s):

Classification:






- international: *H04H1/00; H04L9/14; H04N5/00; H04N5/44; H04N7/16; H04N7/167; H04N7/173; H04H1/00; H04L9/14; H04N5/00; H04N5/44; H04N7/16; H04N7/167; H04N7/173; (IPC1-7): H04H1/00; H04L9/14; H04N5/44; H04N7/16; H04N7/173*

- European: *H04N5/00M4; H04N7/167D; H04N7/16E2*

Application number: JP20010538392T 20001117

Priority number(s): WO2000EP11483 20001117; US19990444495 19991119

Also published as:

 WO0137546 (A2)
 WO0137546 (A3)
 PT1243130 (E)
 ES2284552 (T3)
 EP1243130 (A2)

[more >>](#)

Abstract not available for JP 2003515286 (T)

Abstract of corresponding document: **WO 0137546 (A2)**

Conditional access methods and apparatus are provided for use with digital television receivers and other digital broadband receivers. The methods and apparatus are capable of handling several different digital signal transmission protocols in an automatic and flexible manner. An input unit is provided for analyzing and tagging incoming data bytes so that further processing operations are less dependent on the transmission format being received. A cipher handling unit is provided for adapting in real time the scrambling and descrambling performances to match the requirements of the transmission network and the receiving apparatus. A filtering mechanism is provided for filtering and handling multiple asynchronous data streams in a parallel manner.

~~~~~  
Data supplied from the **espacenet** database — Worldwide

(19) 日本国特許庁 (J P)

## (12) 公表特許公報 (A)

(11) 特許出願公表番号  
特表2003-515286  
(P2003-515286A)

(43) 公表日 平成15年4月22日 (2003. 4. 22)

| (51) Int.Cl. <sup>7</sup> | 識別記号  | F I                        | キーワード* (参考) |
|---------------------------|-------|----------------------------|-------------|
| H 0 4 N 7/16              |       | H 0 4 N 7/16               | A 5 C 0 2 5 |
| H 0 4 H 1/00              |       | H 0 4 H 1/00               | F 5 C 0 6 4 |
| H 0 4 L 9/14              |       | H 0 4 N 5/44               | Z 5 J 1 0 4 |
| H 0 4 N 5/44              |       | 7/173                      | 6 4 0 Z     |
| 7/173                     | 6 4 0 | H 0 4 L 9/00               | 6 4 1       |
|                           |       | 審査請求 未請求 予備審査請求 有 (全 81 頁) |             |

(21) 出願番号 特願2001-538392(P2001-538392)  
 (86) (22) 出願日 平成12年11月17日 (2000. 11. 17)  
 (85) 翻訳文提出日 平成14年5月20日 (2002. 5. 20)  
 (86) 国際出願番号 P C T / E P 0 0 / 1 1 4 8 3  
 (87) 国際公開番号 W O 0 1 / 0 3 7 5 4 6  
 (87) 国際公開日 平成13年5月25日 (2001. 5. 25)  
 (31) 優先権主張番号 0 9 / 4 4 4 , 4 9 5  
 (32) 優先日 平成11年11月19日 (1999. 11. 19)  
 (33) 優先権主張国 米国 (US)  
 (81) 指定国 EP (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), JP, SG

(71) 出願人 エスシーエム・マイクロシステムズ・ゲー  
 エムベーパー  
 ドイツ連邦共和国、85737 イスマニング、  
 オスカー・メスター・シュトラッセ 13  
 (72) 発明者 バンタロン、ルーク  
 アメリカ合衆国、カリフォルニア州  
 94087 サニーバイル、コーディレラス・  
 アベニュー 1396  
 (72) 発明者 シャテニエール、アルノー  
 フランス国、エフ-13600 セレスト、ア  
 レ・ドゥ・ラ・グラネット 31  
 (74) 代理人 弁理士 鈴江 武彦 (外3名)

最終頁に続く

(54) 【発明の名称】 デジタルテレビジョン方法および装置

## (57) 【要約】

条件付きアクセス方法および装置はデジタルテレビジョン受信機および他のデジタル放送受信機で利用されるために与えられる。この方法および装置は自動的にフレキシブルな方法で幾つかの異なるデジタル信号送信プロトコルを処理することができる。さらなる処理動作が受信される送信フォーマットに依存しないように、入力装置は入来するデータバイトを解析しタグ付けするために設けられる。暗号処理装置は送信ネットワークと受信装置の要求を一致させるためにスクランブル性能とデスクランブル性能を実時間に適合するために設けられる。濾波機構は並列方法で多数の非同期データ流を濾波し処理するために設けられる。

**【特許請求の範囲】**

【請求項1】 複数の転送フォーマットのうちの選択された1つであり、複数の暗号フォーマットのうちの選択された1つである信号をネットワークから受信するための受信回路と、

受信された信号を検査し、それに関する転送フォーマットと無関係の情報信号を生成するための回路と、

受信された信号のネットワーク暗号化部分をデスクランブルし、このような部分をエンドユーザに必要なコピー保護暗号化フォーマットにしたがって再スクランブルするためのトランススクランブル回路と、

受信された信号から補助情報を抽出するための濾波回路と、

トランススクランブル回路を制御するために、転送フォーマットと無関係の情報信号と、抽出された補助情報とに応答する制御回路とを具備している適応受信システム。

【請求項2】 複数の転送フォーマットのうちの選択された1つであり複数の暗号フォーマットのうちの選択された1つである信号をネットワークから受信し、

受信された信号を検査し、それに関する転送フォーマットと無関係の情報信号を生成し、

受信された信号のネットワーク暗号化部分をデスクランブルし、このような部分をエンドユーザに必要なコピー保護暗号化フォーマットにしたがって再スクランブルし、

受信された信号から補助情報を抽出し、

デスクランブルおよび再スクランブル動作を制御するために、転送フォーマットと無関係の情報信号と、抽出された補助情報とを使用する適応信号受信方法。

【請求項3】 予め定められたデータ装置でデータを受信し、

受信されたデータ装置を修飾し、

データ装置の暗号化状態を決定し、

暗号化されていないデータの場合には、クリア出力を提供し、

暗号化されたデータの場合には、装置のサイズにしたがって暗号解読機能を行

うステップを含んでいる方法。

【請求項4】 識別データを含んでいるか否かの決定をさらに含んでいる請求項3記載の方法。

【請求項5】 適合試験を行うステップを含んでいる請求項4記載の方法。

【請求項6】 ペイロードバイトが存在するか否かを決定するステップを含んでいる請求項5記載の方法。

【請求項7】 データがスクランブルされているか否かを決定するステップを含んでいる請求項6記載の方法。

【請求項8】 修飾機構と、

マルチビットタグを各受信されたデータバイトへ与えるタグ付け機構とを具備している複数の転送ストリームフォーマットを処理するシステム。

【請求項9】 バイトタイプを決定する機構を含んでいる請求項8記載のシステム。

【請求項10】 バイトがチャンネル識別子を含んでいるか否かを決定する機構をさらに含んでいる請求項9記載のシステム。

【請求項11】 適合試験の実行を含んでいる請求項10記載のシステム。

【請求項12】 ペイロードバイトを識別する機構を含んでいる請求項11記載のシステム。

【請求項13】 受信されたデータがスクランブルされているか否かを決定する機構を含んでいる請求項12記載のシステム。

【請求項14】 受信されたストリームフォーマットに無関係に出力バイト流を発生する機構を含んでいる請求項8記載のシステム。

【請求項15】 選択されたストリームフォーマットにしたがってフォーマットされた入力転送ストリームを受信するように構成されている請求項8記載のシステム。

【請求項16】 選択されたタイプの転送構造を受信するように構成されている請求項8記載のシステム。

【請求項17】 入来するデータバイトを修飾する機構と、

それぞれの入来するデータバイトへタグを割当てる機構とを具備している異な



る転送ストリームフォーマットを受信する機構。

【請求項18】 符号にしたがって受信されたデータバイトを修飾し、それぞれ受信されたデータバイトヘタグを取付けるステップを含んでいる方法。

【請求項19】 選択された転送ストリームフォーマットで信号を生成する1以上の信号送信ソースと通信するように構成されている複数の受信機と、

1以上の受信された信号の転送ストリームを選択し、そこから少なくとも1つのセキュリティ層を除去するように構成されているセキュリティ機構とを具備しているシステム。

【請求項20】 コンテンツ保護のための機構を含んでいる請求項19記載のシステム。

【請求項21】 複数のデコーダをさらに含んでいる請求項19記載のシステム。

【請求項22】 受信された信号を検査してそれらのタイプを決定するように構成されている請求項19記載のシステム。

【請求項23】 受信された信号のデスクランブルを制御するように構成されている請求項22記載のシステム。

【請求項24】 少なくとも1つの予め定められたセキュリティ層にしたがった1以上の信号送信ソースと通信するように構成されている複数の受信機と、少なくとも1つのセキュリティ層を除去するように構成されている機構とを具備しているシステム。

【請求項25】 前記機構は条件付きアクセスモジュールである請求項23記載のシステム。

【請求項26】 ディスプレイ装置を具備している請求項23記載のシステム。

【請求項27】 協動レセプタクルにプラグインするように構成されている請求項23記載のシステム。

【請求項28】 選択された転送ストリームフォーマットで構成されている複数の受信機と、

1以上の転送ストリームを選択するように構成されているセキュリティ機構とを具備しているシステム。

【請求項29】 前記複数の受信機はそれぞれ帯域内チャンネルおよび帯域外チャンネルを含んでいる請求項28記載のシステム。

【請求項30】 前記帯域内および帯域外チャンネルはフィルタバンクと接続されている請求項29記載のシステム。

【請求項31】 スマートカードチャンネルをさらに含んでいる請求項28記載のシステム。

【請求項32】 さらに少なくとも1つのアプリケーションとの通信を可能にするように構成されている請求項29記載のシステム。

【請求項33】 複数の異なるデジタル送信フォーマットの1つでデジタルデータ流を受信する入力信号チャンネルと、

入来するデータ流を信号の送信フォーマットと無関係のセットへ変換する回路と、

送信フォーマットを変換するディスプレイ機構とを具備しているシステム。

【請求項34】 回路は入来するデータバイトの修飾機構と、各データバイトへタグを割当てるタグ付け機構とを含み、受信システムはタグ付けされたデータバイトに応答する回路を含んでいる請求項33記載のシステム。

【請求項35】 修飾機構はパーサ機構を具備している請求項34記載のシステム。

【請求項36】 それぞれ複数の異なるフォーマットの1つで送信される少なくとも2つのデータ流を受信する少なくとも2つの入力チャンネルと、

それぞれの入来するデータ流をフォーマットに無関係の信号のセットへ変換する回路と、

フォーマットに無関係の信号をイメージへ変換する機構と、

フォーマットに無関係のメッセージ信号を感知可能なメッセージに変換するメッセージ処理機構とを具備しているシステム。

【請求項37】 回路は、

第1の修飾機構と、

第1のタグ付け機構と、

第1の信号処理回路と、

第2の修飾機構と、

第2のタグ付け機構と、

メッセージ信号をメッセージ処理機構へ供給するためにタグ付けされたメッセージ信号バイトに応答する第2の信号処理回路とを具備している請求項36記載のシステム。

【請求項38】 それぞれの修飾機構はパーサ機構を具備している請求項37記載のシステム。

【請求項39】 修飾機構と、

タグ付け機構と、

タグ付けされたデータバイトに応答する信号処理機構とを具備しているシステム。

【請求項40】 修飾機構と、

複数ビットのタグを各データバイトへ割当てタグ付け機構とを具備している機構。

【請求項41】 修飾機構はパーサ機構を具備している請求項40記載の機構。

【請求項42】 第1の試験機構と、

タグを示すヘッダバイトを割当てのために第1の試験機構に結合されている第1のタグ付け機構と、

入来する各データバイトを検査してデータがスクランブルされているか否かを決定する第2の試験機構と、

スクランブル状態タグビットを各データバイトへ割当て、データがスクランブルされているならばこのようなビット2進値の一方を与え、データがスクランブルされていないならば他の2進値を与えるように第2の試験機構に結合されている第2のタグ付け機構と、

使用可能なデジタル情報を生成するために、各データバイトおよびその割当てられたタグビットをデータ処理機構へ転送する信号転送回路とを具備している機

構。

【請求項43】 データ装置でデータを受信し、  
データの暗号化状態を決定し、  
暗号化されていないデータの場合には、クリア出力を提供し、  
暗号化されたデータの場合には、受信されたデータ装置のユニットサイズを決定し、決定されたユニットサイズにしたがって暗号解読機能を行い、それによって解読されたデータを与えるステップを含んでいる方法。

【請求項44】 所望のスクランブルフォーマットを選択し、  
セッションキーを選択し、  
選択されたメモリ中に選択されたセッションキーをロードする請求項43記載の方法。

【請求項45】 スクランブルフォーマットを選択するステップを含んでいる請求項43記載の方法。

【請求項46】 放送信号の処理を含んでいる請求項43記載の方法。

【請求項47】 バースト信号の処理を含んでいる請求項43記載の方法。

【請求項48】 選択されたホストと選択されたモジュールとを対にし、  
所望のスクランブルフォーマットを選択し、  
セッションキーを選択するステップを含んでいるスクランブル方法。

【請求項49】 スクランブルフォーマットをDES-ECB、DES-CBC、DES-OFBを含むグループから選択する請求項48記載の方法。

【請求項50】 放送信号の処理を含んでいる請求項49記載の方法。

【請求項51】 バースト信号の処理を含んでいる請求項49記載の方法。

【請求項52】 選択されたホストと選択されたモジュールとを対にし、  
所望のデスクランブルフォーマットを選択し、  
セッションキーを選択するステップを含んでいるデスクランブル方法。

【請求項53】 デスクランブルフォーマットをDVB、DES-ECB、DES-CBC、DES-OFB、MULTI2、3DES-ECB、3DES-CBC、3DES-OFBを含むグループから選択し、DVBはデジタルビデオ放送を意味し、DESはデータ暗号化標準を意味し、ECBは電子コードブッ

クを意味し、CBCはチェンブロック暗号を意味し、OFBは出力フィードバックブロックを意味している請求項52記載の方法。

【請求項54】 デスクランブルのための放送信号の処理を含んでいる請求項52記載の方法。

【請求項55】 デスクランブルのためのパースト信号の処理を含んでいる請求項52記載の方法。

【請求項56】 TS入力データ流を受信するために入力データレジスタによってデスクランブルするステップを含んでいる請求項52記載の方法。

【請求項57】 以下の暗号化フォーマット、即ちDVB、DES-ECB、DES-CBC、DES-OFB、MULTI2、3DES-ECB、3DES-CBC、3DES-OFBの1つをデスクランブルするために複数のデコーダを有するデスクランブラを使用し、DVBはデジタルビデオ放送を意味し、DESはデータ暗号化標準を意味し、ECBは電子コードブックを意味し、CBCはチェンブロック暗号を意味し、OFBは出力フィードバックブロックを意味している請求項52記載の方法。

【請求項58】 入来するデータを処理するために付勢する複数のデコーダの1つを選択するために、デスクランブルフォーマットレジスタおよび関連するデコーダを使用する請求項52記載の方法。

【請求項59】 デスクランブルフォーマットレジスタを使用する請求項52記載の方法。

【請求項60】 前記制御信号はエネーブル信号デコーダによりデコードされる請求項52記載の方法。

【請求項61】 デスクランブルセッションキーによりセッションキーレジスタをロードする請求項60記載の方法。

【請求項62】 デスクランブルキーのロードを含んでいる請求項60記載の方法。

【請求項63】 デスクランブルキーを供給する請求項60記載の方法。

【請求項64】 デコーダを選択し、デスクランブルされたデータ流を生成する請求項63記載の方法。

【請求項65】 スクランブルフォーマットレジスタと、  
制御信号により個々に選択されるように構成されている複数のエンコーダとを  
具備しているスクランブラ。

【請求項66】 エネーブル信号デコーダを含んでいる請求項65記載のスクランブラ。

【請求項67】 スクランブルされたデータ流を生成するように構成されている請求項65記載のスクランブラ。

【請求項68】 スクランブルはスクランブルセッションキーによって制御される請求項65記載のスクランブラ。

【請求項69】 スクランブルセッションキーはマイクロプロセッサから得られる請求項65記載のスクランブラ。

【請求項70】 チャンネル変更を行い、  
デスクランブル機構を選択し、  
セッションキー変更を行い、  
新しいセッションキーをロードするステップを含んでいるスクランブル方法。

【請求項71】 修飾されたパケットセルバイトを受信し、  
受信され修飾されたパケットセルがスクランブルされているか否かを決定し、  
受信され修飾されたパケットセルがスクランブルされていないならば、クリアパケットセルバイトを出力するステップを含んでいる請求項70記載の多数のスクランブル方法。

【請求項72】 修飾されたパケットセルバイトを受信し、  
受信され修飾されたパケットセルがスクランブルされているか否かを決定し、  
受信され修飾されたパケットセルがスクランブルされていないならば、クリアパケットセルバイトを出力するステップを含んでいる方法。

【請求項73】 受信され修飾されたパケットセルがスクランブルされているならば、フルブロック状態の決定が行われる請求項72記載の方法。

【請求項74】 フルブロック決定が否定であるならば、減少されたサイズのブロック決定が行われる請求項73記載の方法。

【請求項75】 コピー保護状態を決定し、

コピー保護状態決定が否定であるならば、クリア情報を出力する請求項72記載の方法。

【請求項76】 コピー保護状態決定が肯定であるならば、ブロック状態の決定が行われ、

ブロック状態にしたがって動作が行われる請求項72記載の方法。

【請求項77】 第1のサイズに対するブロック決定が否定であるならば、短いブロック決定が行われ、

短いブロック決定が肯定であるならば、短いブロック動作が行われる請求項72記載の方法。

【請求項78】 データの修飾されたバイトを受信し、  
受信され修飾されたバイトがスクランブルされているか否かを決定し、  
受信され修飾されたバイトがスクランブルされていないならば、クリア情報が出力されるステップを含んでいる方法。

【請求項79】 コピー保護に関して決定が行われ、  
決定が否定であるならば、クリア情報を発生する請求項78記載の方法。

【請求項80】 パケット内の受信されたデータバイトを修飾し、  
タグをそれぞれ受信されたデータバイトに取付け、  
所望のスクランブルフォーマットを選択し、  
セッションキーを選択するステップを含んでいる方法。

【請求項81】 各バイトのタイプを決定するために、各バイトを検査するステップをさらに含んでいる請求項80記載の方法。

【請求項82】 さらに、バイトがチャンネル識別子を含んでいるか否かを決定するステップを含んでいる請求項80記載の方法。

【請求項83】 適合フィールド試験を行う請求項80記載の方法。

【請求項84】 バイトがペイロードバイトであるか否かを決定する請求項80記載の方法。

【請求項85】 バイトのデータがスクランブルされているか否かを決定する請求項80記載の方法。

【請求項86】 受信された特定の転送ストリームフォーマットと独立して

いる出力バイト流を発生する請求項80記載の方法。

【請求項87】 位置および値にしたがって受信されたデータバイトを処理する修飾機構と、

受信された各データバイトヘタグを与えるタグ付け機構と、

スクランブルフォーマットレジスタと、

スクランブルフォーマットレジスタへロードされる複数ビットの制御信号により個々に選択されるように構成されている複数のエンコーダとを具備しているシステム。

【請求項88】 エネーブル信号デコーダと、

選択されたエンコーダの出力においてスクランブルされたデータ流を生成するように構成されている機構とを含んでいる請求項87記載のシステム。

【請求項89】 スクランブルは複数ビットのスクランブルセッションキーにより制御される請求項87記載のシステム。

【請求項90】 スクランブルセッションキーはマイクロプロセッサから得られる請求項87記載のシステム。

【請求項91】 それぞれ受信されたバイトを検査する機構を含んでいる請求項87記載のシステム。

【請求項92】 バイトがチャンネル識別データを含んでいるか否かを決定する機構をさらに具備している請求項87記載のシステム。

【請求項93】 適合試験を実行する機構を含んでいる請求項87記載のシステム。

【請求項94】 バイトがペイロードバイトであるか否かを決定する機構を含んでいる請求項87記載のシステム。

【請求項95】 バイト中のデータがスクランブルされているか否かを決定する機構を含んでいる請求項87記載のシステム。

【請求項96】 特定の転送ストリームフォーマットに依存しない出力バイト流を生成する機構を含んでいる請求項87記載のシステム。

【請求項97】 選択された転送ストリームフォーマットにしたがってフォーマットされた入力転送ストリームを受信するように構成されている請求項87



記載のシステム。

【請求項98】 選択された転送構造を受信するように構成されている請求項87記載のシステム。

【請求項99】 受信されたデータバイトを修飾し、  
修飾されたデータバイトがスクランブルされているか否かおよびこれがコピー保護されるべきか否かを示すために受信された各データバイトにタグを取付けるステップを含んでいる複数の信号フォーマットを処理する方法。

【請求項100】 修飾機構と、  
タグを各データバイトに割当ててタグ付け機構と、  
スクランブルフォーマット機構とを具備しているシステム。

【請求項101】 選択された信号フォーマットで信号を発生する1以上の信号送信ソースと通信するように構成されている複数の受信機と、

ブロックタイプに応じてセキュリティ層を除去するように受信された信号流を選択するように構成されているセキュリティ機構とを具備しているシステム。

【請求項102】 前記セキュリティ機構はコンテンツ保護を予め定められた信号流へ与える請求項101記載のシステム。

【請求項103】 1以上の信号流を選択するように構成されている複数のデコーダをさらに含んでいる請求項101記載のシステム。

【請求項104】 前記セキュリティ機構は受信された信号を分類するように構成されている請求項101記載のシステム。

【請求項105】 前記セキュリティ機構はデスクランブル動作を制御するように構成されている請求項101記載のシステム。

【請求項106】 秘密保護されるストリームを受信するように構成されている複数の受信機と、

ブロックタイプにしたがって、ネットワーク分配セキュリティ層をそこから除去するように構成されているセキュリティ機構とを具備しているシステム。

【請求項107】 前記セキュリティ機構は除去可能な素子である請求項106記載のシステム。

【請求項108】 前記セキュリティ機構は協動レセプタクルにプラグイン

するように構成されている請求項106記載のシステム。

【請求項109】 選択された転送ストリームフォーマットで通信するように構成されている複数の受信機と、

1以上の受信された信号転送ストリームを選択し、そこからネットワーク分配セキュリティ限定を除去するように構成されているセキュリティ機構とを具備しているシステム。

【請求項110】 前記複数の各受信機は帯域内チャンネルおよび帯域外チャンネルを含んでいる請求項109記載のシステム。

【請求項111】 前記帯域内および帯域外チャンネルはフィルタバンクと接続されている請求項109記載のシステム。

【請求項112】 さらに、スマートカードチャンネルを含んでいる請求項109記載のシステム。

【請求項113】 異なるフォーマットにしたがってスクランブルされたデジタルデータ信号を受信するための入力回路と、

受信された信号の暗号化フォーマットを識別する機構と、

受信されたデータ信号をデスクランブルするデスクランブル機構と、

デスクランブルされたデータ信号を再スクランブルするスクランブル機構とを具備しているシステム。

【請求項114】 デジタルテレビジョン受信システムを含んでいる請求項113記載のシステム。

【請求項115】 可視イメージを生成するためのテレビジョンディスプレイ機構を含んでいる請求項113記載のシステム。

【請求項116】 ビデオテープレコーダを含んでいる請求項113記載のシステム。

【請求項117】 受信されたデータ信号は第1のデータ暗号化フォーマットにしたがってスクランブルされ、第2のデータ暗号化フォーマットにしたがって再スクランブルされる請求項113記載のシステム。

【請求項118】 第1のデータ暗号化フォーマットはDVB、DES-ECB、DES-CBC、DES-OFB、MULTI2、3DES-ECB、3

D E S - C B C、3 D E S - O F Bから選択された1つのフォーマットであり、D V Bはデジタルビデオ放送を意味し、D E Sはデータ暗号化標準を意味し、E C Bは電子コードブックを意味し、C B Cはチェンブロック暗号を意味し、O F Bは出力フィードバックブロックを意味し、第2のデータ暗号化フォーマットはD E Sフォーマットである請求項1 1 7記載のシステム。

【請求項1 1 9】 スクランブル機構は、受信された信号の暗号化フォーマットとは異なるスクランブルされたデータ信号を生成する請求項1 1 8記載のシステム。

【請求項1 2 0】 受信されたデータ信号は第1の複数の異なるデータ暗号化フォーマットのうちの特定の1つのフォーマットにしたがってスクランブルされ、第2の複数の異なるデータ暗号化フォーマットのうち特定の1つのフォーマットにしたがってスクランブルされるスクランブルデータ信号を生成する請求項1 1 8記載のシステム。

【請求項1 2 1】 受信されたデータ信号のスクランブルシーケンスはスクランブルキーによって制御される請求項1 1 8記載のシステム。

【請求項1 2 2】 デスクランブル機構はデータ信号をデスクランブルする複数のデコーダ機構とデコーダ選択機構とを具備している請求項1 1 8記載のシステム。

【請求項1 2 3】 異なるデータ暗号化フォーマットにしたがってスクランブルする複数のエンコーダ機構と、クリア情報をスクランブルするために特定のエンコーダ機構を選択するエンコーダ選択機構とを含んでいる請求項1 1 8記載のシステム。

【請求項1 2 4】 第1のタイプの暗号で暗号化された情報を解読し、第2のタイプの暗号によって前記情報を再度暗号化する方法。

【請求項1 2 5】 修飾された情報を受信し、修飾された情報がスクランブルされているかを決定し、スクランブルされていないならば、スクランブルされていない情報をスクランブルせずに転送するステップを含んでいる方法。

【請求項1 2 6】 情報を受信するためにチャンネルを選択し、

デスクランブル機構を選択し、  
デスクランブルを可能にするためのデスクランブルセッションキーを決定する  
ステップを含んでいる方法。

【請求項127】 決定された機構およびキーにしたがってデスクランブル  
を行う請求項126記載の方法。

【請求項128】 選択されたスクランブル機構による再スクランブルを含  
んでいる請求項127記載の方法。

【請求項129】 選択された条件付きアクセスモジュールまたはカードと  
選択されたモジュールとを対にし、

コピー保護機構を選択し、  
スクランブルセッションキーを決定するステップを含んでいる方法。

【請求項130】 多数フォーマットの転送ストリームを受信する回路と、  
パケットまたはセル内の位置にしたがってデータバイトを識別する機構と、  
パケットまたはセル内の値にしたがってデータバイトを識別し、一致が検出さ  
れたとき一致指示信号を発生する機構と、

一致指示信号に応答するデータ抽出機構とを具備している機構。

【請求項131】 異なるユーザアプリケーションを識別するためのパター  
ンメモリ装置を含んでいる請求項130記載の機構。

【請求項132】 並列する多数のセクション後に処理を行う複数のフィル  
タセルを含んでいる請求項130記載の機構。

【請求項133】 アクチブセルの特別なセクション長を増加するために幾  
つかのフィルタセルを減勢する機構を含んでいる請求項130記載の機構。

【請求項134】 関連するペイロードの前の特別なセクションと一致する  
データバイトを抽出するシフトレジスタを含んでいる請求項130記載の機構。

【請求項135】 受信されたデジタル信号内の異なる予め規定されたデジ  
タルパターンを検出する検出器と、

異なる予め規定されたデジタルパターンにそれぞれ関連するデータバイトを異  
なるエンド使用位置へ転送する回路とを具備しているシステム。

【請求項136】 エンド使用位置は異なるアプリケーションプログラムで

ある請求項135記載のシステム。

【請求項137】 複数のデジタルデータ転送ストリームを受信し、異なるエンド使用を意図している転送ストリームセグメントを分離する複数のフィルタ装置と、

分離されたセグメントを受信する複数の短期間の記憶装置と、

長期間の記憶装置と、

時間共有方法で短期間の記憶装置を長期間の記憶装置へ結合するマルチプレクサ機構とを具備しているシステム。

【請求項138】 記憶される前に私有暗号キーにしたがって信号をスクランブルし、

再生されるときこの同一の私有暗号キーにしたがって記録された信号をデスクランブルするステップを含んでいる方法。

【請求項139】 保護される信号を受信し、

受信された信号を局部的に生成される暗号キーにしたがってスクランブルし、

スクランブルされた信号を信号記憶媒体に記録し、

記憶された信号を再生し、

再生された信号を局部的に発生された暗号キーにしたがってデスクランブルし

、

デスクランブルされた信号をエンドユーザシステムに供給するステップを含んでいる方法。

【請求項140】 保護される信号を受信し、

受信された信号を局部的に生成された暗号キーにしたがってスクランブルし、

スクランブルされた信号を信号記憶媒体に記録するステップを含んでいる方法

。

【請求項141】 記憶された信号を再生し、

再生された信号を予め定められた暗号キーと同一の暗号キーにしたがってデスクランブルし、

デスクランブルされた信号をエンドユーザシステムに供給するステップを含んでいる方法。

【請求項142】 予め定められたキーにしたがってスクランブルされるスクランブルバージョンを生成するために記憶される信号に応答するスクランブラ機構と、

保護されたコピーを生成するためにスクランブルされた信号を記憶媒体に記録する記録機構と、

記憶媒体に記憶されたスクランブルされた信号を再生する再生機構と、

再生された信号を予め定められたキーにしたがってデスクランブルするためにその信号に応答するデスクランブル機構と、

デスクランブルされた信号をエンドユーザへ供給する回路とを具備しているシステム。

【請求項143】 信号はデジタル信号である請求項142記載のシステム。

【請求項144】 信号はデジタルテレビジョン信号である請求項142記載のシステム。

【請求項145】 信号はデジタルビデオ信号である請求項142記載のシステム。

【請求項146】 信号はデジタルオーディオ信号である請求項143記載のシステム。

【請求項147】 記憶媒体は取外し可能な記憶装置である請求項143記載のシステム。

【請求項148】 記憶媒体はコンピュータ記憶媒体である請求項142記載のシステム。

【請求項149】 記憶媒体は磁気媒体である請求項142記載のシステム。

【請求項150】 信号記憶媒体は光記憶媒体である請求項142記載のシステム。

【請求項151】 信号記憶媒体は集積回路メモリ装置である請求項142記載のシステム。

【請求項152】 予め定められた暗号キーにしたがってスクランブルされ

たスクランブルバージョンを生成するために記憶される信号に応答するスクランブラ機構と、

セキュリティ保護され記憶されたコピーを生成するためにスクランブルされた信号を信号記憶媒体に記録する記録機構とを具備しているシステム。

【請求項153】 信号記憶媒体に記憶されたスクランブルされた信号を再生する再生機構と、

再生された信号を予め定められた暗号キーにしたがってデスクランブルするためにその信号に応答するデスクランブル機構と、

デスクランブルされた信号をエンドユーザシステムへ供給する回路を具備しているシステム。

【請求項154】 受信されスクランブルされた信号のクリアコピーバージョンを生成するために、その信号をデスクランブルするためにその信号に応答するデスクランブラ機構と、

クリアコピー信号を私有暗号キーにしたがってスクランブルするためにその信号に応答するスクランブラ機構と、

私的にスクランブルされた信号の私的記憶コピーを生成するためその信号を信号記憶媒体へ供給する回路を具備しているシステム。

【請求項155】 デスクランブラ機構は送信された暗号キーにしたがって受信された信号をデスクランブルする請求項154記載のシステム。

【請求項156】 送信された暗号キーは条件付きアクセスシステムによって使用される同一の条件付きアクセス暗号キーである請求項154記載のシステム。

【請求項157】 信号記憶媒体に記録された私的にスクランブルされた信号を再生し、このような私的にスクランブルされた信号は私的暗号キーにしたがってスクランブルされているプレイバック機構と、

その信号のクリアコピーバージョンを生成するために、私的暗号キーにしたがってその信号をデスクランブルするデスクランブラ機構と、

クリアコピー信号を条件付きアクセスシステムにより使用されるコピー保護暗号キーにしたがってスクランブルするためにその信号に応答するスクランブラ機

構と、

コピー保護されたスクランブルされた信号をエンドユーザシステムへ供給する回路とを具備しているシステム。

【請求項158】 データを受信するマルチ転送システムと、  
前記受信されたデータを処理するマルチスクランブルシステムと、  
ユーザコンテンツを制御データから分離するためにエンドユーザアプリケーションにしたがって前記受信されたデータを濾波するマルチ濾波システムとを具備しているマルチフォーマット信号システム。

【請求項159】 複数のフォーマットのうちの1つを有しスクランブルを受ける制御およびコンテンツ情報を処理する方法において、

制御およびコンテンツ情報を受信し、修飾し、修飾状態にしたがってタグ付けし、

決定されたデスクランブル動作に対する修飾タグを使用し、

制御情報をコンテンツ情報から分離するステップを含んでいる方法。

【請求項160】 複数の暗号化フォーマットのうちの選択された1つである信号をネットワークから受信する受信回路と、

受信された信号のネットワーク暗号化部分をデスクランブルし、このような部分をエンドユーザに必要なコピー保護暗号化フォーマットにしたがって再スクランブルするためのトランススクランブル回路と、

受信された信号から補助情報を抽出するためのフィルタ回路と、

トランススクランブル回路を制御するために、抽出された補助情報に応答する制御回路とを具備している適合性受信システム。

【請求項161】 複数の転送フォーマットのうちの選択された1つであり複数の暗号フォーマットのうちの選択された1つである信号をネットワークから受信するための受信回路と、

受信された信号を検査し、それに関する転送フォーマットに無関係な情報信号を生成するための回路と、

受信された信号のネットワーク暗号化部分をデスクランブルし、このような部分をエンドユーザに必要なコピー保護暗号化フォーマットにしたがって再スクラ



ンプルするためのトランススクランブル回路と、

トランススクランブル回路を制御するために、転送フォーマットに無関係な情報信号に応答する制御回路とを具備している適合性受信システム。

【請求項162】 複数の転送フォーマットのうちの選択された1つであり、複数の暗号フォーマットのうちの選択された1つである信号をネットワークから受信するための受信回路と、

受信された信号を検査し、それに関する転送フォーマットに無関係な情報信号を生成するための回路と、

受信された信号のネットワーク暗号化部分をデスクランブルし、このような部分をエンドユーザに必要なコピー保護暗号化フォーマットにしたがって再スクランブルするためのトランススクランブル回路と、

受信された信号から補助情報を抽出するためのフィルタ回路とを具備している適合性受信システム。

**【発明の詳細な説明】****【0001】****【発明の属する技術分野】**

本発明はデジタルテレビジョンシステムおよびサービスに関し、特にこのようなシステムおよびサービスで使用するための条件付きアクセス方法および装置に関する。

**【0002】****【従来の技術】**

デジタルテレビジョンは公共での人気が高まっている新しい技術である。さらに関心のある特徴の1つはいわゆる“高画質テレビジョン（HDTV）”の導入であり、この放送は最近、米国連邦通信委員会により承認された。HDTVは既存の“普通画質”テレビジョンシステムにより与えられるよりも高い品質および画質のテレビジョンイメージを与える。

**【0003】**

デジタルテレビジョンの別の高い重要な特徴は、ビデオオンデマンドプログラミング、ペイ・パー・ビュー映画、スポーツイベント、対話式ビデオゲーム、ホームショッピング能力、高速度インターネットアクセス等の関連するサービスの提供である。ホームテレビジョンセットは将来の媒体を不要にするきわだった情報およびサービスに急速になりつつある。

**【0004】****【発明が解決しようとする課題】**

知られているように、テレビジョンサービスは現在、地上ベースの無線タイプの放送送信、ケーブルネットワーク送信、宇宙衛星送信により通信されている。受信を支払加入者に限定するために、ケーブルおよび衛星のプロバイダが送信をスクランブルし、カスタマが受信された信号をスクランブルから復元するために特別なセットトップ制御ボックスの使用を必要とすることが普通に行われる。このようなスクランブルおよびセットトップボックス技術は関連するサービスのプロバイダによっても所望される。これまでの問題は、各プロバイダがその固有の特有で独占的なセットトップ制御ボックスを開発していることである。したがっ

て、多数のプロバイダから信号を受信して使用するために、多数のセットトップ制御ボックスの使用を必要とする。これは最良の状態ではなく、米国連邦通信委員会はいわゆる多数のプロバイダからコンテンツを受信して処理することのできるユニバーサルなセットトップボックスを与えるためのいわゆる“オープン”セットトップボックスによる方法を推奨している。残念ながら、これを実行し、同時に権限のないユーザに対するサービスを阻止して種々のサービスプロバイダを保護するのに必要なセキュリティ制御特性を与えることは容易ではない。

#### 【0005】

##### 【課題を解決するための手段】

本発明は“ユニバーサルな”セットトップ制御ボックスを提供するために使用される実効的でフレキシブルな適応した受信システムを提供する。この受信システムはマテリアルの権限のない使用に対する高度の保護を与える方法で送信されたプログラムマテリアルへの条件付きのアクセスを許可する。この適応性受信システムはネットワークからの信号、例えば複数の転送フォーマットうちの選択された1つであり複数の暗号フォーマットのうちの選択された1つである信号を受信するための受信回路を含んでいる。このシステムはまた、受信された信号を検査し、それに関係する転送フォーマットに無関係に情報信号を発生するための回路を含んでいる。このシステムはさらに受信された信号のネットワーク暗号化部分をデスクランブルし、このような部分をエンドユーザに必要なコピー保護暗号化フォーマットにしたがって再スクランブルするためのトランススクランブル回路を含んでいる。受信された信号から補助情報を抽出するための濾波回路が設けられ、システムはさらに、転送フォーマットに無関係の情報信号と、トランススクランブル回路を制御するために抽出された補助情報に応答する制御回路を含んでいる。

#### 【0006】

##### 【発明の実施の形態】

本発明をより良好に理解するために、その他のおよび更なる利点およびその特徴と共に、添付図面と共に以下の詳細な説明を参照にして説明する。本発明の技術的範囲は特許請求の範囲に記載されている。

図1を参照すると、1以上の放送信号送信ネットワークへ接続された1以上の受信機10を有するデジタル広帯域受信システムの一般的なブロック図が示されている。典型的に信号伝送ネットワークは地上ベースの無線周波数タイプの放送ネットワーク、ケーブルネットワーク、宇宙衛星信号送信ネットワーク、広帯域電話ネットワーク等を含んでいる。送信しようとするアナログ情報信号（例えばビデオ信号、オーディオ信号またはデータ信号）は送信目的の特別なデジタル転送ストリームフォーマットに変換される。典型的な転送ストリームフォーマットはMPEGフォーマット、DSSフォーマット、ATMフォーマットである。MPEGフォーマットはモーションピクチャエキスパートグループにより開発されたデータ伝送フォーマットである。好ましい形態のMPEGはMPEG-2であり、これはISO/IEC標準規格13818に規定されている。“DSS”はデジタル衛星システムを表し、幾つかの衛星オペレータにより使用されるデジタル信号の送信で使用するために開発されたフォーマットを意味する。“ATM”は非同期転送モードを表す。デジタル信号プロトコルは固定速度とパースト情報との両者をブロードバンドデジタルネットワークで効率的に転送するためのものである。ATMデジタル流は“セル”と呼ばれる固定長のパケットからなる。

#### 【0007】

各受信機10はその受信された信号を復調し、復調された信号をセキュリティ機構11へ与える。セキュリティ機構11はエンドユーザが信号受信の資格を有するならば、受信された信号転送ストリームの1以上を選択し、そこからネットワーク分配セキュリティ層を除去する。ネットワークセキュリティ機構11はまたそれを必要とする任意の信号流へコンテンツ保護を適用する。結果的な信号はデコーダ12へ供給され、このデコーダ12は1以上の信号流を選択し、選択された各信号流をデコードして所望のビデオ、オーディオ、およびデータ信号を再度生成し、それらは代わりに1以上のディスプレイ装置13および1以上の記録装置14へ与えられる。典型的なディスプレイ装置はテレビジョンセットおよびテレビジョンおよびコンピュータモニタを含んでいる。典型的な記録装置はVCRタイプのビデオレコーダおよび種々のタイプのコンピュータメモリ装置を含んでいる。セキュリティ機構11は受信された1つまたは複数の信号を検査し、それらのタイプを決

定し、それらのデスクランブルを制御する。セキュリティ機構11は必要とされる条件が満たされるならば、受信された信号のアンスクランブルバージョンへのアクセスを可能にする。

#### 【0008】

通常のようなデジタルテレビジョンプログラミングに加えて、図1の受信システムはまた種々の関連する通信サービスを受信し処理する。関連するサービスの例としてはビデオオンデマンドプログラミング、ペイ・パー・ビュー映画およびスポーツイベント、対話式ビデオゲーム、ホームショッピングサービス、高速度インターネットアクセス等である。認められるように、これらの関連するサービスのためのデータ信号と制御信号はいわゆる“帯域外”チャンネルの方法により供給される。

#### 【0009】

図2AおよびBは図1の装置の異なる方法のパッケージを示している。特に図2Aの(a)は受信機10、セキュリティ機構11、デコーダ12がネットワーク特定セットトップボックス15内に位置されている場合を示している。1つの例では、セキュリティ機構11はセットトップボックス15内に埋設されるか、その内部に永久的に取り付けられる。典型的な使用では、セットトップボックス15はディスプレイ装置13の上部に配置される。

#### 【0010】

図2Aの(b)は条件付きアクセスモジュール(CAM)17により表されている更新可能で除去可能なアドオンセキュリティ機構を有するオープンタイプのセットトップボックス16を示している。条件付きアクセスモジュール17は図2Aの(a)のセキュリティ機構11により行われるセキュリティ機能を実行する。アクセスモジュール17はホストセットトップボックス16の協動するレセプタクルまたはソケットにプラグインされるように構成されている取外し可能なプラグインタイプである。図2Aの(a)のように、セットトップボックス16はディスプレイ装置13の上部に位置するように設計されている。

#### 【0011】

図2Bの(a)はセットトップボックス機能がテレビジョン受信機のキャビ

ネット18の内部、即ちディスプレイ装置または受像管13を収容するキャビネット内に位置されている場合を示している。条件付きアクセスモジュール17はキャビネット18の外部からアクセス可能な協働するレセプタクルにプラグインするように構成されている。図2Bの(a)は条件付きアクセスモジュール17により表されている更新可能なアドオンセキュリティ機構を有する一体化されたテレビジョンセットを表している。

#### 【0012】

図2Bの(b)は主要な装置が別々のコンポーネントタイプのキャビネットまたはボックス19a-19dに位置されているケースを表している。条件付きアクセスモジュール17は受信機ボックス19aまたはデコーダボックス19bに取り外し可能にプラグインされてもよく、またはその代わりにボックス19aと19bとの間に接続されている小さいコネクタ装置の一部であってもよい。図2Bの(b)の構造は特に家庭用を目的とするコンポーネントタイプの娯楽センタで有効である。

#### 【0013】

図3を参照すると、本発明の1実施形態の概念図が示されている。図に示されるように、受信装置は帯域内チャンネル20と帯域外チャンネル21を含んでおり、これらは遠隔位置の放送局から入来する信号を受信するように構成されている。帯域内チャンネル20はデジタルテレビジョン信号等の主要なユーザ信号を処理する。他方、帯域外チャンネル21はビデオオンデマンドコマンド、セキュリティデータ、e-コマーストランザクション等の関連するサービスのためのデジタル信号を処理する。チャンネル20と21の両者はフィルタバンク23により種々のアプリケーションプログラム22と通信し、フィルタバンク23は受信された信号内の種々の規定されたデジタルパターンを検出し、適切な1つのアプリケーション22との接続を設定するためそれに応答する。

#### 【0014】

図3の装置はまたスマートカードSCとアプリケーションプログラム22との間に通信を行うためのスマートカードチャンネル24を含んでいる。データチャンネル25はホスト装置中に位置するCPU（中央処理装置）例えばセットトップボ

ックス (S T B) 16と、アプリケーションプログラム22との間に通信を行う。拡張されたチャンネル26はネットワークからホストC P Uへ、またはその逆方向で帯域外チャンネルによってネットワークデータを転送するために設けられている。

#### 【0015】

図4を参照すると、図2 Aの (b) のホスト装置またはセットトップボックス16および条件付きアクセスモジュール17の代表的な形態の内部指令を詳細に示している。図4に示されているように、信号コネクタ29はセットトップボックス16を、信号を供給する通信ネットワークに接続する。この信号路29は帯域内受信機30と帯域外受信機31へ延在する。通信ネットワークはマルチチャンネルシステムであり、主要なビデオおよびオーディオ信号を伝送するチャンネルは“帯域内”チャンネルとラベルを付けられ、関連するサービスのための信号を伝送するチャンネルは“帯域外”チャンネルと呼ばれる。セットトップボックス16は、ネットワーク放送センタに位置するデジタルデータプロバイダへ信号を返送するためにさらに帯域外送信機32を含んでいる。

#### 【0016】

受信機30と31の出力に現れるデジタル信号は条件付きアクセスモジュール17へ与えられる。主要なビデオおよびオーディオ信号はセットトップボックス16のデコーダ33へ返送され、そこからデジタルT Vディスプレイ13に与えられる。セットトップボックス16はマイクロプロセッサ装置34を含み、これは特に制御信号をデコーダ33へ与える。メモリ装置36はマイクロプロセッサ装置34へ結合され、特にマイクロプロセッサ装置34により使用される種々の制御ルーチンおよびアプリケーションプログラム機能の記憶を行う。マイクロプロセッサ装置34とメモリ36はセットトップボックス16のC P U機能を与える。

#### 【0017】

図4の条件付きアクセスモジュール (C A M) 17は帯域内受信機30と帯域外受信機31から出力デジタル信号を受信する転送ストリーム (T S) コプロセッサ40を含んでおり、帯域外受信機31からの信号は帯域外デコーダ41により与えられる。転送ストリームコプロセッサ40はまたT Vディスプレイ13のためのデジタル

ビデオおよびデジタルオーディオ信号をデコーダ33へ供給する。条件付きアクセスモジュール17はさらにマイクロプロセッサ装置42および関連するメモリ装置43を含んでいる。これらの装置42および43は条件付きアクセスモジュール17に対するCPU機能を与える。アプリケーションプログラム22の主要部分はメモリ43に記憶されている。データチャンネル44はCAMマイクロプロセッサ装置42とホストマイクロプロセッサ装置34との間に直接通信リンクを与える。CAMマイクロプロセッサ装置42はまたデジタルメッセージおよび情報をネットワーク放送センタへ返送できる。これはホストセットトップボックス16の帯域外エンコーダ45と帯域外送信機32により行われる。取外し可能なスマートカード28は制御情報をそこに供給するためにマイクロプロセッサ装置42へ接続されるように構成されている。

#### 【0018】

拡張されたチャンネルはネットワーク放送センタがホストマイクロプロセッサ装置34との間で通信することを可能にするために設けられている。この拡張されたチャンネルの入来ブランチは帯域外受信機31に結合されて帯域外デコーダ41まで延在する信号路47を含んでいる。この入来ブランチはデコーダ41、転送ストリームコプロセッサ40、マイクロプロセッサ42、マイクロプロセッサ42からホストマイクロプロセッサ34まで配線された信号路49を含んでいる。この拡張されたチャンネルからの出力ブランチは、ホストマイクロプロセッサ34から帯域外エンコーダ45へ接続された信号路50により与えられる。

#### 【0019】

図5を参照すると、図4の条件付きアクセスモジュール(CAM)17の転送ストリーム(TS)のコプロセッサ40とマイクロプロセッサ装置42の詳細なブロック図が示されている。図5に示されているように、転送ストリーム(TS)のコプロセッサ40はそれぞれ帯域内受信機30と帯域外受信機31から並列タイプのデジタル入力信号TS入力1とTS入力2を受信する転送ストリーム(TS)入力装置52を含んでいる。直列タイプのデジタル信号TS入力3は帯域外受信機31から受信される。入力装置52からの出力信号はさらに処理するため暗号バンク54に与えられる。暗号バンク54はTS出力装置55とフィルタバンク56の入力に接続さ



れる2つの並列タイプの出力流を発生する。暗号バンク54内でのマルチプレクサ選択により、暗号バンク54への2つの入力流の一方は内部暗号プロセッサによって処理され、他の入力流は単にTS出力装置55とフィルタバンク56へバイパスされる。TS出力装置55からのTS出力信号はセットトップボックス16のデコーダ33に与えられる。

#### 【0020】

転送ストリーム入力装置52は複数の異なる転送ストリームフォーマットを受信できる多数のデータ転送機構を含んでいる。特に、これはそれらの複数バイトのデータパケットの位置および値にしたがって入来するデータバイトを受信し修飾する修飾機構を含んでいる。TS入力装置52はさらに複数ビットのタグを各データバイトへ割当てするタグ付け機構を含み、そのようなタグは修飾プロセスの結果により決定された特有値を有する。タグビットはデータバイトをさらに処理するのを容易にするために使用される。

#### 【0021】

マイクロプロセッサ装置42は典型的に高速度転送モードで動作する32ビットARMシステムバスASBに接続されているARM7マイクロプロセッサ60を含んでいる。ASBバスにはメモリインターフェース装置61、アドレスデコーダ装置62、調停装置63、読取り専用メモリ(ROM)装置64に接続されている。メモリインターフェース61はマイクロプロセッサ装置42に関連する外部メモリ43に接続されている。

#### 【0022】

マイクロプロセッサ60はVLSI周辺バスVPBにより転送ストリームコプロセッサ40および種々の他の装置と通信する。このVPBバスはバス間のブリッジ装置65と高速度ASBバスによりマイクロプロセッサ60に接続されている。ASBバスは高速度転送用に使用され、VPBバスは低い優先順位の通信に使用される。コプロセッサ40のフィルタバンク56がその出力データに対して外部メモリ43への直接および高速度アクセスを必要とするとき、これもASBバスに接続される。結果として、ASBバスには3つのマスター、即ちマイクロプロセッサ60と、フィルタバンク56の2つのチャンネルが存在する。3つのマスター間の仲裁

は調停装置63により管理される。比較により、V P Bバスは1つのマスター、即ちマイクロプロセッサ60だけを有する。

### 【0023】

アドレスレコーダ62はA S Bバス上のデータの正しいターゲットを選択するためにA S Bバスのアドレスビットをデコードする。典型的なターゲットはメモリインターフェース61、R O M 64、および種々の周辺装置、ならびにA S Bバスに接続されている他の装置である。割込み制御装置66はマイクロプロセッサ60に対する割込み機能を与え、タイマ67は種々のタイミング機能を与える。転送ストリームコプロセッサ40中の各装置は制御および状態目的で低い優先順位のV P Bバスに結合される。またV P Bバスには拡張されたチャンネル装置68と、データチャンネル装置69と、P C M C I A インターフェース70とが接続されている。周辺インターフェース装置71はV P Bバスと1以上の周辺装置との間のインターフェースを与える。例えば、スマートカードインターフェースコネクタ構造72は図4で示されている取外し可能なスマートカード28と接続するために設けられている。直列インターフェース73は直列タイプの周辺装置P Dへ接続するために設けられてもよい。

### 【0024】

図6は本発明の帯域外チャンネル特徴の代表的な形態の構成を示している。この帯域外チャンネル特徴は図4で示されている帯域外受信機31から帯域外信号O B入力を受信する帯域外チャンネルデコーダ41を含んでいる。デコーダ41の出力はさらに濾波動作するために転送ストリームコプロセッサ40により与えられる。帯域外チャンネルの出力または送信機部分はA T Mエンコーダ45、送信バッファ46、チャンネルエンコーダ48を含み、チャンネルエンコーダ48は図4で示されている帯域外送信機32へ帯域外出力信号O B出力を供給する。A T Mエンコーダ45はマイクロプロセッサ装置42に関連するV P B周辺バスからその入力信号を受信する。送信されるデータはマイクロプロセッサ装置42中に位置するアプリケーションプログラム、または拡張されたチャンネル路50によりセットトップボックス16から受信されるデータのいずれかにより供給される。このデータはA T Mエンコーダ45によりA T Mセルへセグメント化される。これらのセルは一時的にバ

ッファ46に記憶される。ネットワークが幾つかの送信スロットを条件付きアクセスモジュール17へ許可するとき、送信バッファ46はチャンネルエンコーダ48により空にされ、帯域外送信機32によりネットワーク放送センタへ送信される。

#### 【0025】

図7は本発明のマイクロプロセッサ対マイクロプロセッサデータチャンネルの特徴を示している。この特徴はCAMマイクロプロセッサ装置42がホストマイクロプロセッサ装置34との間で直接通信することを可能にする。マイクロプロセッサ装置42はデータチャンネル44aによりデータをマイクロプロセッサ装置34へ送信する。ホスト装置34はデータチャンネル44bによりデータをCAMマイクロプロセッサ装置42へ送信する。

#### 【0026】

図8は図5のスマートカードインターフェース72の詳細を示している。スマートカード28はスマートカード読取り装置86へ挿入されるように構成され、スマートカード28から受信されたデータは入力バッファ87によりマイクロプロセッサ装置42に関連する周辺バスVPBへ供給される。マイクロプロセッサ装置42からのデータはVPBバス、出力バッファ88、スマートカード読取り装置86によりスマートカード28に供給される。代表的な実施形態では、スマートカード読取り装置86はPCMCIAカード読取り装置である。PCMCIAはパーソナルコンピュータメモ리카ード国際協会を表している。これは標準的なメモ리카ードインターフェースを規定するため1989年に設立された非営利の貿易協会である。スマートカード読取り装置86はインターフェース標準規格にしたがっている。

#### 【0027】

図9を参照すると、図5の転送ストリーム入力装置52の代表的な形態の構造を詳細に示している。TS入力1とTS入力2信号は入力レジスタ130と131に与えられる。直列入力信号TS入力3は直列—並列変換器132へ与えられ、これはその信号を直列形態から並列形態へ変換する。変換器132の並列出力はさらに入力レジスタ133に与えられる。レジスタ130、131、133の出力は3：2マルチプレクサ134に接続されている。このマルチプレクサ134は3つの入力のうち2つを選択し、選択された入力の一方をTS1 F I F O装置135に供給し、他

方の選択された入力をTS2カウンタ装置136へ供給する。FIFO135はTS1パーサ137への入力を与え、カウンタ136はTS2パーサ138への入力を与える。パーサ137と138はそれぞれの信号流をバイト対バイトのベースで解析し、複数ビットのタグを各データバイトへ割当てて。特に、各パーサ137と138は複数バイトのデータパケットの位置と値にしたがって入来するデータバイトを受信し、修飾する修飾機構を含んでいる。代表的な実施形態では、5ビットのタグが各データバイトで発生され、それに取付けられる。この5ビットのタグの値は修飾機構により実行される修飾プロセスによって決定される。パーサ137と138は、各データ流が接続される特定の出力路TSaまたはTSbを決定する選択パーサ139に接続されている。

#### 【0028】

図10を参照すると、図5の暗号バンク54の代表的な形態の構成を詳細に示している。暗号バンク54は図9のTS入力装置52から2つの信号流TSaとTSbを受信する。暗号バンク54からの2つの出力バス74と75はTS出力装置55とフィルタバンク56に接続されている。したがって、暗号バンク54は2つの入力流と2つの出力流とを有する。マルチプレクサ76、77、78による選択によって、1つの入力流が暗号プロセッサ79により処理され、一方、他の入力流は単にその対応する1つのマルチプレクサ77、78の出力へバイパスされる。マルチプレクサ76、77、78はそれぞれVPBバスにより獲得された選択信号S1、S2、S3によって制御される。

#### 【0029】

マルチプレクサ設定の第1のセットでは、TSa流はマルチプレクサ76により暗号プロセッサ79へ転送され、暗号プロセッサ79の出力はマルチプレクサ77により暗号バンク54のTS出力1バス74へ転送される。この同じケースでは、第2の入力データ流TSbはマルチプレクサ78によりTS出力2バス75へ供給される。マルチプレクサ設定の第2のセットでは、状態は反転される。TSbデータ流はマルチプレクサ76により暗号プロセッサ79へ供給され、結果的に処理された信号はマルチプレクサ78によりTS出力2バス75へ供給される。第2のケースでは、TSa入力データ流はマルチプレクサ77によりTS出力1バス74へ供給される。

。暗号プロセッサ79は保護されたデータ流T S<sub>p</sub>とクリアデータ流T S<sub>c</sub>との両者を出力する。マルチプレクサ77と78は一方または他方のこれらのデータ流を選択するが、両者とも選択することはない。

### 【0030】

図11を参照すると、図10の暗号プロセッサ79の主要な構成素子が示されている。図11に示されているように、暗号プロセッサ79は条件付きアクセスデスクランブラ80とコピー保護スクランブラ81とを含んでいる。デスクランブラ80はクリアコピー出力信号T S<sub>クリア</sub>を発生するためにスクランブルされた入来するデジタル信号をデスクランブルする。デスクランブラ80は以下の暗号化フォーマット、即ち欧州で使用されているDVBスーパースクランプリングフォーマット、米国で使用されているDESおよび3DESデータ暗号化標準フォーマット、日本で使用されているMULTI2フォーマットをデスクランブルすることができる。コピー保護スクランブラ81は条件付きアクセスモジュール17の出力でデータコンテンツが盗まれることを防止するためにデスクランブラ80の出力でクリアコピー信号を再スクランブルするために使用される。スクランブラ81はDESデータ暗号化標準スクランプリング方法を使用する。

### 【0031】

図12は図11の条件付きアクセスデスクランブラ80の代表的な形態の構成の詳細を示している。図12のデスクランブラ80は図10のマルチプレクサ76からT S入力データ流を受信するための入力データレジスタ140を含んでいる。デスクランブラ80はまた以下の暗号化フォーマット、即ちDVB、DES-ECB、DES-CBC、DES-OFB、MULTI2、3DES-ECB、3DES-CBC、3DES-OFBの1つをデスクランブルするための1組の8つのデコーダ141-148を含んでいる。その他の暗号化フォーマットは適切な付加的なデコーダを設けることによって適合されることができる。前述の記号文字は以下の意味を有する。

| 記号文字 | 説明            |
|------|---------------|
| DVB  | デジタルビデオ放送（欧州） |
| DES  | データ暗号化標準（米国）  |

E C B      電子コードブック  
C B C      チェーンブロック暗号  
O F B      出力フィードバックブロック

E C B、C B C、O F BフォーマットはD E Sおよび3 D E Sフォーマットの既知の変形である。

#### 【0032】

デスクランブルフォーマットレジスタ150 および関連するデコーダ151 は、入来するデータ流を処理するために付勢される主要なデコーダ 141—148 の1つを決定する。デスクランブルフォーマットレジスタ150 は使用されるデコーダを指定する複数ビットの制御信号をV P Bバスによりロードされる。この制御信号は1つのみの出力ラインを付勢するためにエネーブル信号デコーダ151 によりデコードされる。したがってデコーダ 141—148 のうちの選択された1つだけが付勢され、または任意の与えられたデータ転送ストリームに対して使用される。

#### 【0033】

また、入来するデータ流をデスクランブルする方法を選択された1つのデコーダ 141—148 へ伝えるデスクランブルセッションキーをセッションキーレジスタ152 にロードすることも必要である。このデスクランブルキーはV P Bバスによりレジスタ152 へロードされる。レジスタ152 は次いで各デコーダ 141—148 へデスクランブルキーを与え、これはデスクランブルフォーマットレジスタ150 中の制御信号により選択されるデコーダにより使用される。デコーダ 141—148 の選択された1つの出力で現れるデスクランブルされたデータはクリアまたはアンスクランブルされた出力信号T S クリアまたはT S cを与えるために出力データレジスタ153 へ与えられる。

#### 【0034】

図13を参照すると、図11のコピー保護スクランブラ81の代表的な形態の構成の詳細が示されている。図13で示されている実施形態では、デスクランブラ81は以下の3つの暗号化フォーマット、即ちD E S—E C B、D E S—C B C、D E S—O F Bのうちの1つにしたがってデスクランブラ80からT S クリア信号をエンコードするための1組の3つのエンコーダ 155、156、157を含んでい

る。所望ならば、他のスクランブルフォーマットが使用されてもよい。エンコーダ 155-157 からの所望の 1 つのエンコーダの選択はスクランブルフォーマットレジスタ158 へロードされる複数ビット 7 の制御信号により実現される。この制御信号は選択された 1 つの出力ラインを付勢するためにエネーブル信号デコーダ 159 を制御し、その出力ラインはエンコーダ 155-157 の異なるものに接続されている。選択されたエンコーダの出力に現れるスクランブルされたデータ流はコピー保護された出力信号保護された T S または T S p を与えるため出力データレジスタ160 に与えられる。選択されたエンコーダで行われる実際のスクランブルプロセスはセッションキーレジスタ161 へロードされる複数ビットのスクランブルセッションキーにより制御される。このスクランブルセッションキーは V P B バスによりマイクロプロセッサ装置42から得られる。

#### 【0035】

図14を参照すると、図5のフィルタバンク56の代表的な形態の構成が示されている。フィルタバンク56は受信されるデータパケットのタイプを決定するために入来するデータ流を検査する。所望のパケットが識別されるとき、そのデータペイロードはその後、メモリ43の適切な位置に記憶され、その特定のパケットタイプに割当てられる。このようにして、入来するデータはアプリケーションまたは意図された使用にしたがって濾波されるか分類されてもよい。特に、フィルタバンク56は異なる転送ストリームフォーマットを伝送する 2 つの入力 F L T 入力 1 と F L T 入力 2 を有する。例えば、第 1 の入力 F L T 入力 1 は帯域内受信機 30 からの帯域内チャンネル出力に接続されてもよく、そのデータ流は M P E G パケットフォーマットを使用することが想定される。第 2 の入力 F L T 入力 2 は帯域外受信機 31 からのデータ流を受信でき、この帯域外チャンネルのデータ信号は非同期転送モード (A T M) セルフフォーマットであることが想定される。

#### 【0036】

フィルタバンク56は異なるデータ流を処理するように独立して設定されることができ、4 つのフィルタ装置 90-93 を含んでいる。このアーキテクチャはアプリケーションタイプに応じて濾波リソースのフレキシブルな調節を可能にする。例えば条件付きアクセスモジュールが A T S C ータイプの新型のテレビジョンサ

ービス（例えば高画質テレビジョン）をサポートするように設定される場合には、4つのフィルタ装置90-93は帯域内チャンネルに同調される。他方で、オープンケーブルタイプの動作では、3つまでのフィルタ装置がIPおよび所有者メッセージを集めるため帯域外チャンネルを処理するように設定されることができ、第4のフィルタ装置は帯域内コマンド信号を処理するため帯域内チャンネルに同調されたままでなければならない。フィルタ装置90-93の出力はスイッチング信号S4により制御されるマルチプレクサ94によってマイクロプロセッサのASBバスへ選択的に接続される。

### 【0037】

図15は図11のフィルタ装置90-93の1つの代表的な形態の構成を詳細に示している。各フィルタ装置90-93はこの同一構造である。図12のフィルタ装置は選択信号S5により2つの入力的一方を選択するように設定されたマルチプレクサ95により2つの入力FLT入力1とFLT入力2の一方に同調される。選択された入力信号流は図9のTS入力装置52でデータバイトに取付けられた複数ビットのタグにしたがって、データバイトを予め濾波するタイプフィルタ96に与えられる。濾波されたバイトはその後、フィルタセル97a-97hのアレイに記憶される。検出することが望まれる予め記録された信号パターンはパターンメモリ98に記憶され、フィルタセル97a-97hに与えられる。パターンの一致が生じたとき、対応するフィルタセルはシフトレジスタ99をロードする。完全なメッセージはCAMマイクロプロセッサ装置42に関連するメモリ装置43中に記憶するためにシフトレジスタ99から抽出される。

### 【0038】

図16の(A)は本発明で使用されることが出来る1つの形態のPCMCIAスマートカード読取り装置の平面図である。図16の(B)は左端面図であり、図16の(C)は右端面図であり、図16の(D)はカード読取り装置の側面図である。記号文字PCMCIAはパーソナルコンメモリカード国際協会を表している。これは標準的なメモリカードインターフェースを規定するため1989年に形成された非営利の貿易協会である。図16のスマートカード読取り装置はプラスチックメモリカード、またはプラスチッククレジットカードとほぼ同じ寸



法のスマートカードを受けると構成された金属ケース100 を含んでいる。ケース100 は I S O 標準規格7816にしたがっている。使用において、スマートカードはケース100 に挿入され、ケース100 はセットトップボックス16の適切なコネクタレセプタクルに挿入される。

#### 【0039】

図17は本発明により使用されてもよい別の形態の P C M C I A カード読取り装置の斜視図である。図17の読取りケース101 は短い延長部を有し、したがって、全体的な長さがさらに短い。図18は使用されてもよいさらに別の形態のカード読取り装置を示している。図18の読取りケース102 はいわゆるデュアル読取りケースであり、2つの異なるスマートカードを受けると構成されている。

#### 【0040】

図19、20、21は本発明により処理されることができ異なるタイプのデータ転送ストリームのパケットフォーマットを示している。図19は M P E G データ流パケットのフォーマットを示している。図20は D S S データ流パケットのフォーマットを示し、図21は A T M データ流セルのフォーマットを示している。M P E G フォーマットはモーションピクチャエキスパートグループにより開発されたデータ伝送フォーマットである。好ましい形態の M P E G は M P E G - 2 であり、これは I S O / I E C 標準規格13818 に規定されている。記号文字 “D S S” はデジタル衛星システムを表し、幾つかの衛星オペレータにより使用されるデジタル信号の送信で使用するために開発されたフォーマットを意味する。記号文字 “A T M” は非同期転送モードを表す。デジタル信号プロトコルは固定速度とバースト情報との両者をブロードバンドデジタルネットワークで実効的に転送するためのものである。A T M デジタル流は “セル” と呼ばれる固定長のパケットからなる。各セルは 53 の 8 ビットバイトを含み、5 バイトのヘッダと 48 バイトの情報ペイロードからなる。米国で使用が承認されたデジタルテレビジョン信号標準規格はビデオ、オーディオ、データ信号をパケット化し多重化するために M P E G - 2 転送ストリームフォーマットを使用する。

#### 【0041】

MPEGパケットは全体の長さが188バイトであり、4バイトのヘッダフィールドと、ゼロバイトから数バイトまで長さが変化する可変長適合フィールドを含んでいる。パケットの残りはペイロードバイトからなる。DSSパケットは全体の長さが130バイトであり、3バイトのヘッダフィールドと、比較的小さい長さの随意的な可変長適合フィールドとを含んでいる。DSSパケットの残りはペイロードバイトからなる。

#### 【0042】

図22は本発明の多数のデータ転送特徴の一般特性を説明するフローチャートである。新しく受信された各データバイト（ブロック103）はそのデータパケットの位置および値にしたがって検査され修飾される（ブロック125）。検査されたバイトはその後、複数ビットのタグでタグ付けされ（ブロック126）、タグの値は修飾プロセスの結果により決定される（ブロック125）。結果的にタグ付けされたバイトはその後修飾されたバイトとして送られる（ブロック124）。本発明の実施形態では、図22により説明されるプロセスは図9で示されているTS入力装置52により実行される。受信されたデータバイトの修飾およびタグ付けはパーサ137と138により実行される。

#### 【0043】

図23を参照すると、図22の方法の代表的な構成の詳細なフローチャートを示している。この図23の多数の転送方法により条件付きアクセスモジュール17はMPEG、ATM、DSS転送ストリームフォーマットを処理することが可能である。入来する各データバイトはそのパケット内の位置および値にしたがって修飾される。この修飾機構は5ビットのタグを各データバイトへ取付け、そのタグはさらにバイトを処理するために必要な全ての情報を含んでいる。各新しいバイトの修飾は図23のブロック103で開始し、このブロックは新しいバイトの受信を表している。バイトは最初にこれがヘッダバイトであるか否かを決定するように検査される（ブロック104）。イエスであるならば、その後それがチャンネル識別（ID）データを含んでいるか否かに関する決定が行われる（ブロック105）。回答がイエスならば、そのバイトは“011”値を有する3ビットのタグ部分が割当てられる（ブロック106）。これがチャンネルIDではないならば

、バイトは“010”値を有する3ビットのタグ部分が割当てられる（ブロック107）。タグ全体は5ビットのタグであることに注意する。他の2ビットの目的を簡単に説明する。

#### 【0044】

ブロック104の決定が、新しいバイトがヘッダバイトではないことを決定したならば、バイトは一連のさらなる非ヘッダバイト検査を受ける。ブロック108により表される第1の試験はバイトがゼロバイトであるか否かを決定する。イエスであるならば、ブロック109により示されるように“000”コードを有する3ビットタグを割当てられる。回答がノーならば、バイトはブロック110により表される適合フィールド試験へ進行する。バイトが適合フィールドバイトであるならば、ブロック111により表されるようにタグ値“101”を割当てられる。適合フィールドバイトではないならば、ブロック112の試験はそれがテーブル識別（ID）バイトであるか否かを決定するために行われる。イエスであるならば、バイトはブロック113により表されるように“110”値を有する3ビットのタグを割当てられる。ノーであるならば、バイトはそれがセクション長インジケータバイトであるか否かを決定するためブロック114で試験される。イエスであるならば、ブロック115により示されるように“001”の3ビットのタグ値を割当てられる。ノーであるならば、バイトはペイロード決定ブロック116へ進行する。これは唯一残された代わりのブロックであるので、バイトはペイロードバイトであることが決定され、ブロック117で示されるように“111”値を有する3ビットのタブ部分を与えられる。

#### 【0045】

タグの最初の3ビット部分を割当てた後、新たに受信されたバイトは決定ブロック118により示されるように、そのデータがスクランブルされているかまたはクリアされているかを決定するために試験される。スクランブルされているならば、タグの第4のビット、即ちSCRビットは1に設定される。スクランブルされていないならば、SCRビットは0に設定される。バイトはその後ブロック121により示されているように、これがヘッダフィールドまたはペイロードフィールドの最後のバイトであるかを決定するために試験される。最後のバイトであ

るならば、LTBビット（5ビットタグの第5のビット）は1に設定され（ブロック122）、ノーであるならば、LTBビットは0に設定される（ブロック123）。これは修飾プロセスを完了し、ステップ124の修飾された出力バイトは条件付きアクセスモジュール17でさらに処理される状態である。

#### 【0046】

図23の修飾プロセスは出力バイト流を発生し、この出力バイト流は条件付きアクセスモジュール17に運ぶ特定の転送ストリームフォーマットにもはや依存しない。したがって、条件付きアクセスモジュール17は複雑性を最少にして効率的な方法で種々の異なる転送ストリームフォーマットの処理を可能にされる。説明した構成はMPEG、DSSおよびATM転送ストリームフォーマットをサポートするが、他のパケットタイプまたはセルタイプの転送構造の処理にも容易に拡張されることができる。

#### 【0047】

図24は図5の暗号バンク装置の別の実施形態を示している。

#### 【0048】

図25は本発明にしたがった入力流インターフェースに対するタイミング図である。

#### 【0049】

図26は本発明にしたがった出力流インターフェースに対するタイミング図である。

#### 【0050】

現時点で、本発明の好ましいと考えられる実施形態について説明したが、種々の変形および変更が本発明の技術的範囲を逸脱せずにここで行われてもよく、それ故、本発明の技術的範囲内に入る全てのこのような変形および変更をカバーすることを意図していることは当業者には明白であろう。

#### 【図面の簡単な説明】

##### 【図1】

送信されたイメージの権限のない表示を阻止するためのセキュリティ機構を有するデジタルテレビジョン受信システムのブロック図。

**【図2 A】**

図1の装置をパッケージする異なる方法のブロック図。

**【図2 B】**

図1の装置をパッケージする異なる方法のブロック図。

**【図3】**

本発明の1実施形態の概念図。

**【図4】**

図2 Aのセットトップボックスおよび条件付きアクセスモジュールの代表的な形態の内部構造の詳細図。

**【図5】**

図4の条件付きアクセスモジュールの転送ストリームのコプロセッサおよびマイクロプロセッサ装置の詳細なブロック図。

**【図6】**

本発明の帯域外チャンネル特徴の代表的な形態の構成図。

**【図7】**

本発明のマイクロプロセッサ間のデータチャンネル特徴の代表的な形態の構成図。

**【図8】**

本発明のスマートカードチャンネル特徴の代表的な形態の構成図。

**【図9】**

図5の転送ストリーム（TS）入力装置の代表的な形態の構成図。

**【図10】**

図5の暗号バンク装置の代表的な形態の詳細な構成図。

**【図11】**

図10の暗号プロセッサの一般的形態の構成図。

**【図12】**

図11の条件付きアクセスデスクランブラの代表的な形態の詳細な構成図。

**【図13】**

図11のコピー保護スクランブラの代表的な形態の詳細な構成図。

**【図14】**

図5のフィルタバンク装置の代表的な形態の構成図。

**【図15】**

図14の1つのフィルタ装置の詳細な構成図。

**【図16】**

本発明により使用されることのできるPCMCIAスマートカード読取り装置の1つの形態の平面図と、そのカード読取り装置の左端面図および右端面図と、その1側面を示した側面図。

**【図17】**

本発明により使用されることのできる別の形態のPCMCIAカード読取り装置の斜視図。

**【図18】**

使用されることのできるさらに別の形態のカード読取り装置の斜視図。

**【図19】**

本発明により処理されることのできる異なるタイプのデータ転送ストリームのためのパケットフォーマット図。

**【図20】**

本発明により処理されることのできる異なるタイプのデータ転送ストリームのためのパケットフォーマット図。

**【図21】**

本発明により処理されることのできる異なるタイプのデータ転送ストリームのためのパケットフォーマット図。

**【図22】**

本発明の多数のデータ転送特徴の説明に使用されるフローチャート。

**【図23】**

図22の方法の代表的な実行の詳細なフローチャート。

**【図24】**

図5の暗号バンク装置の別の実施形態の構成図。

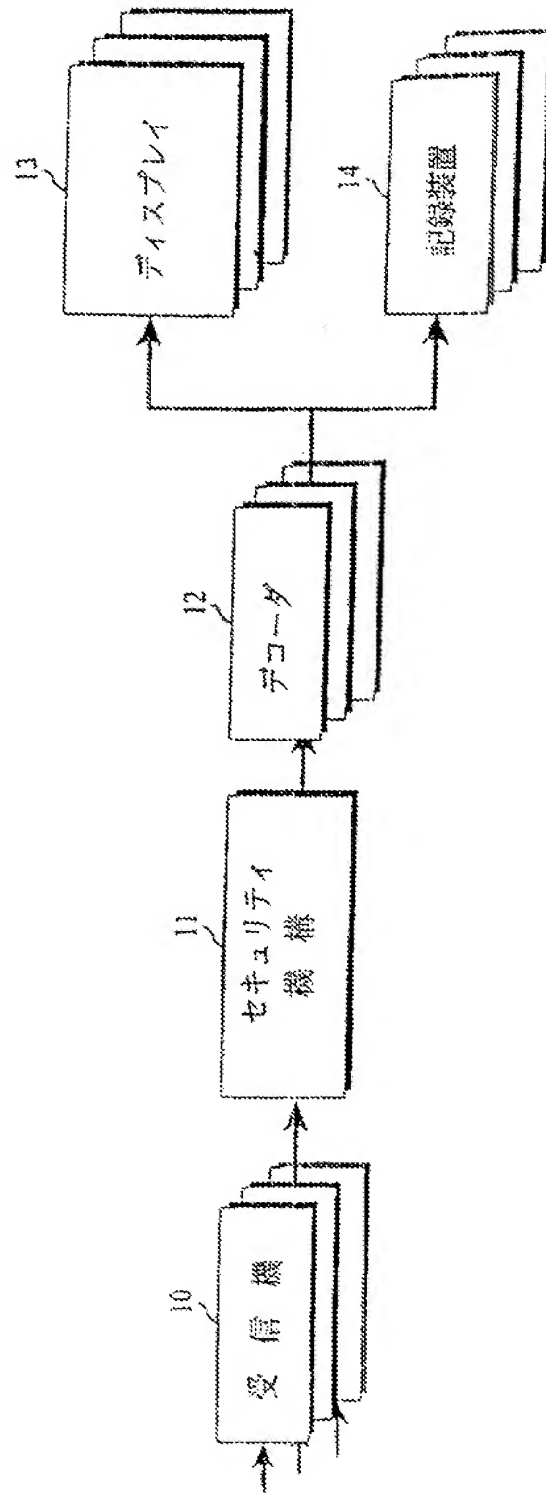
**【図25】**

本発明にしたがった入力流インターフェースのタイミング図。

【図26】

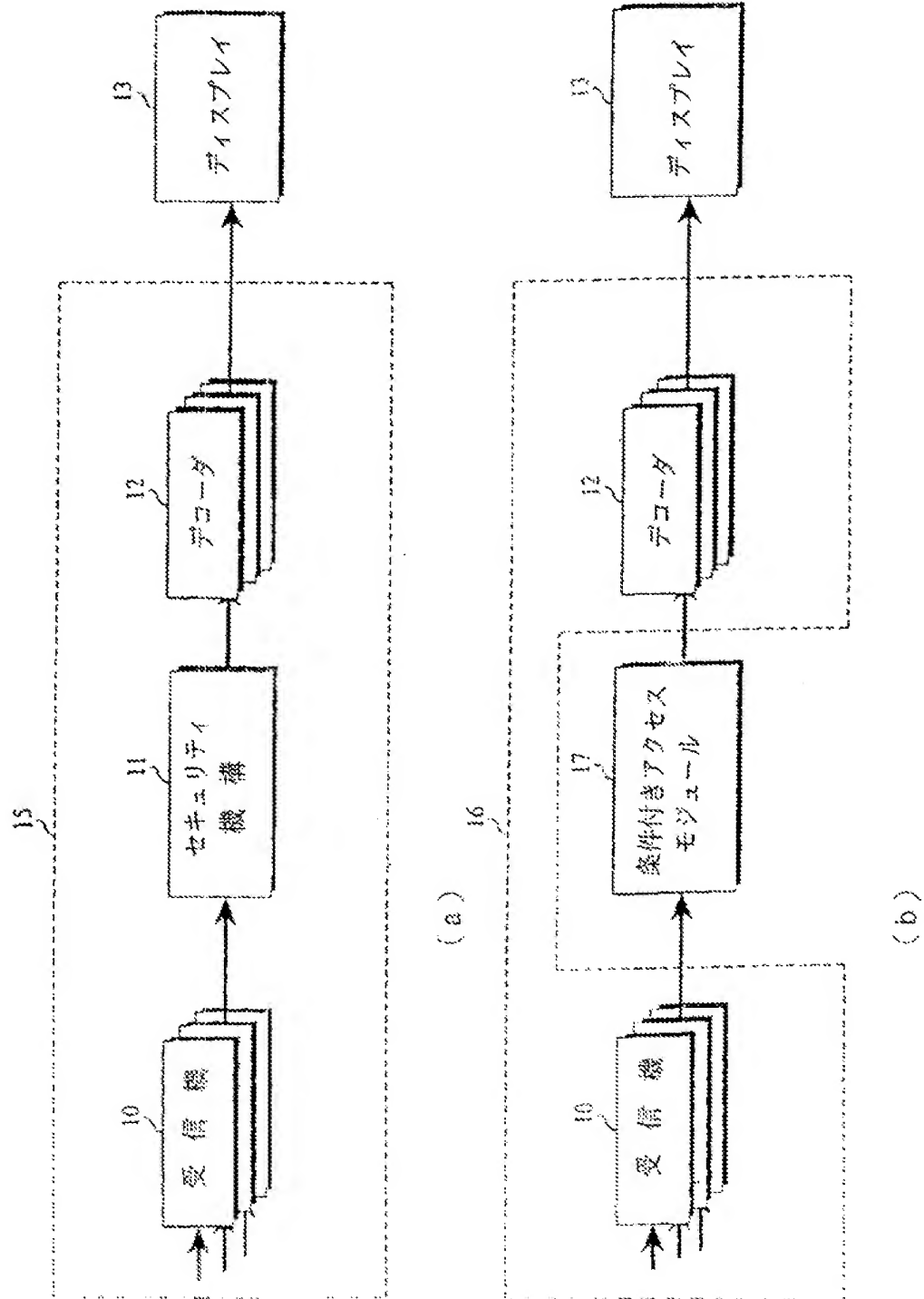
本発明にしたがった出力流インターフェースのタイミング図。

【図1】

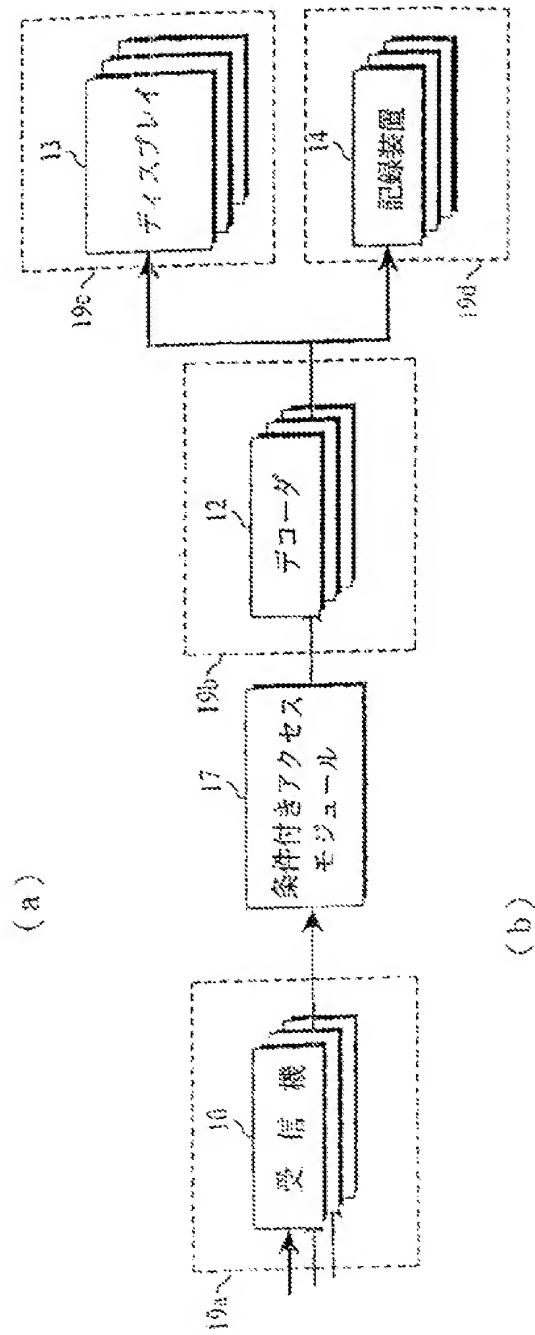
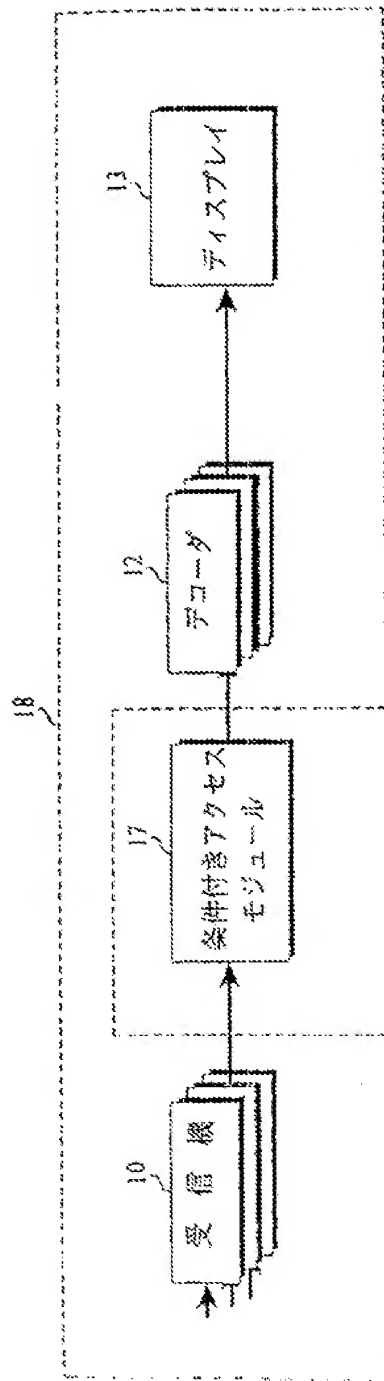




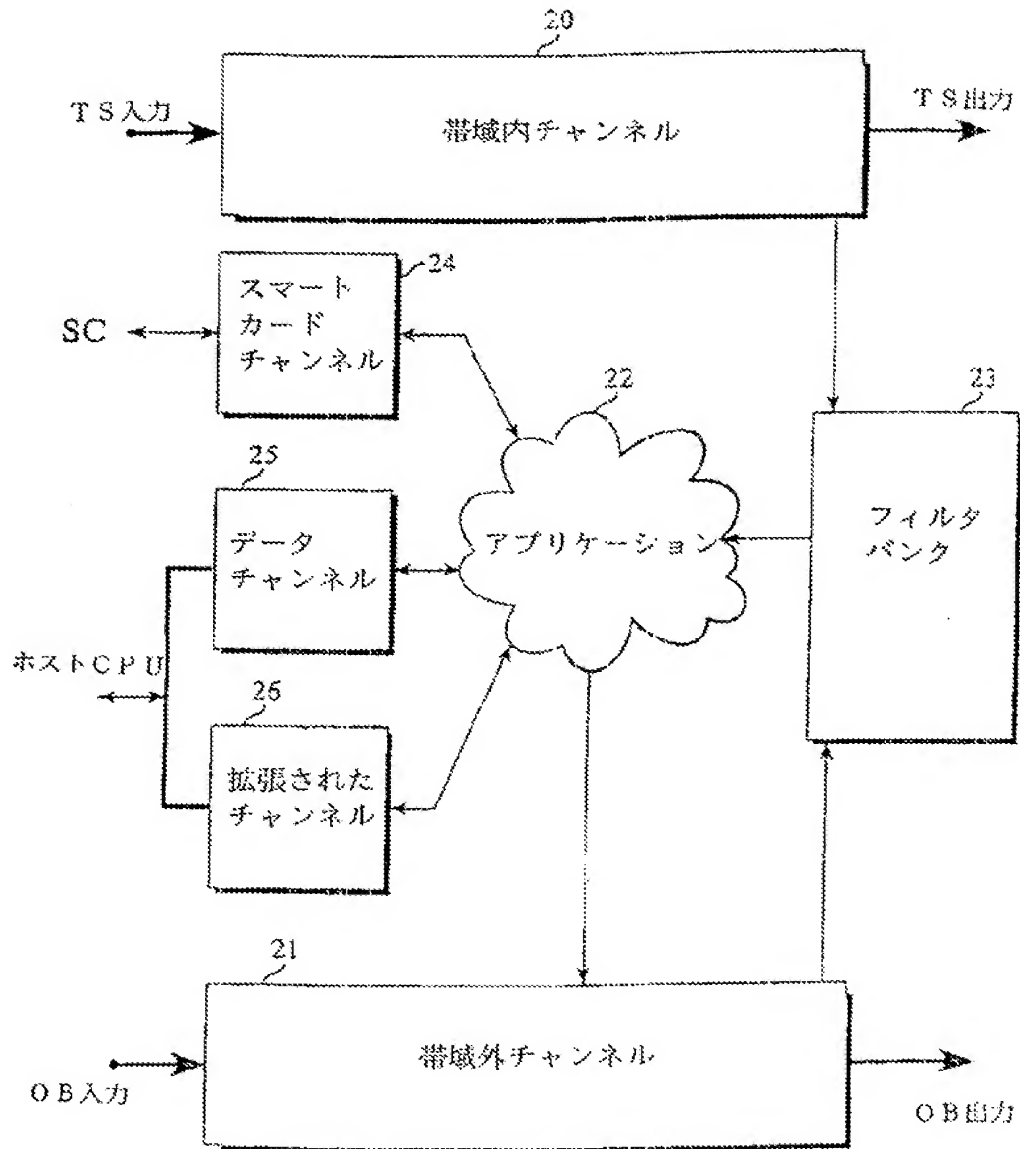
【図2A】



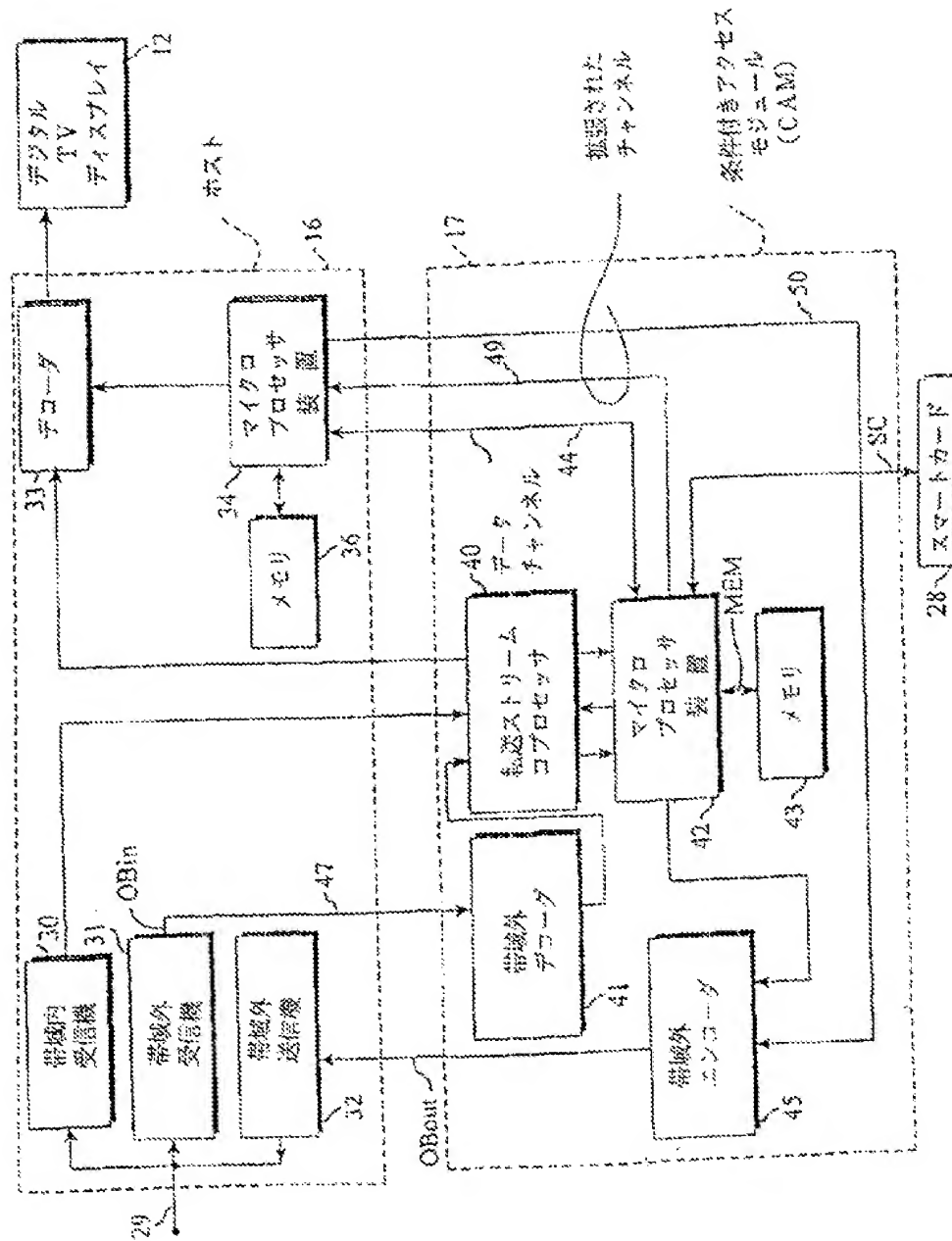
【図2B】



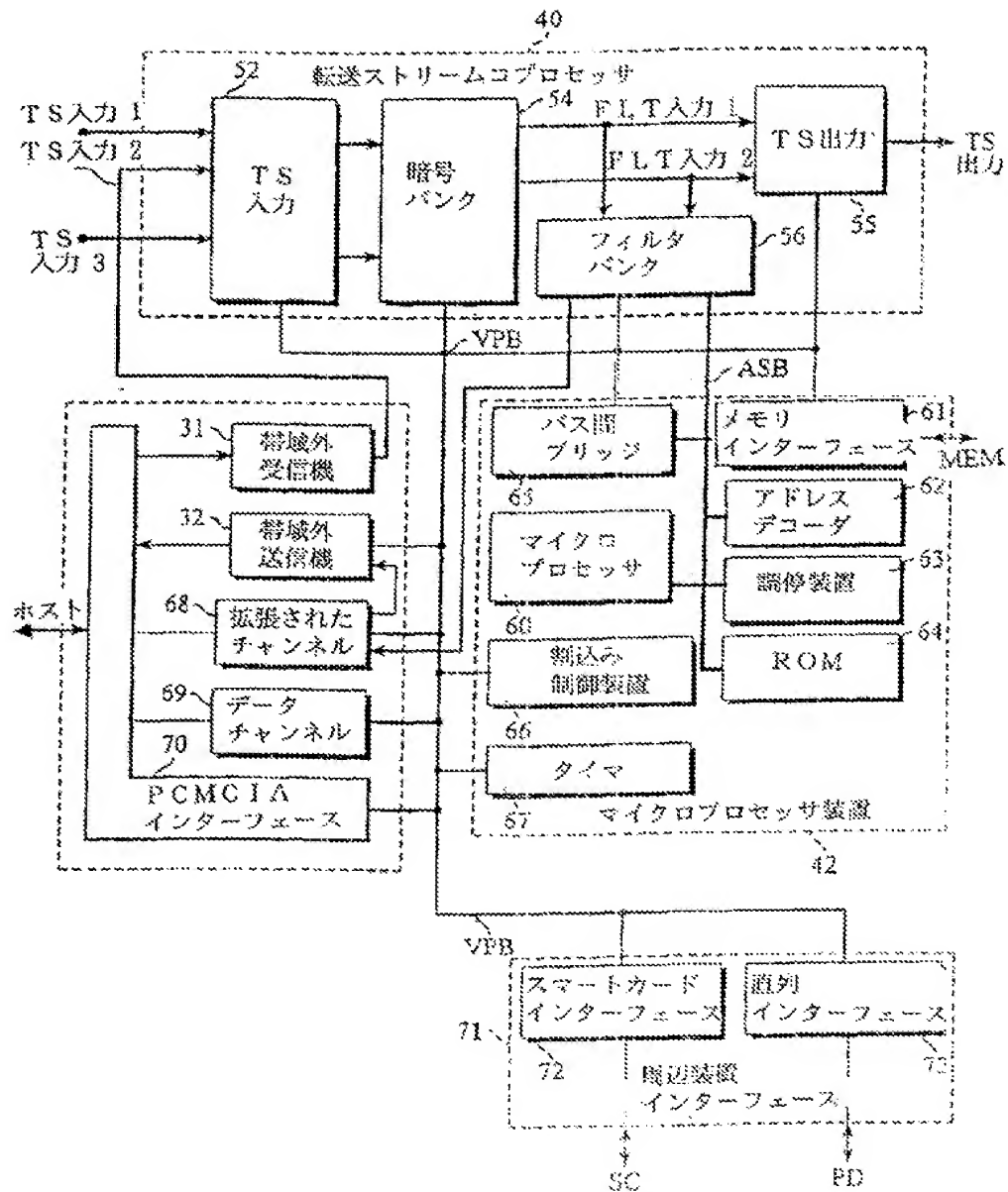
【図3】



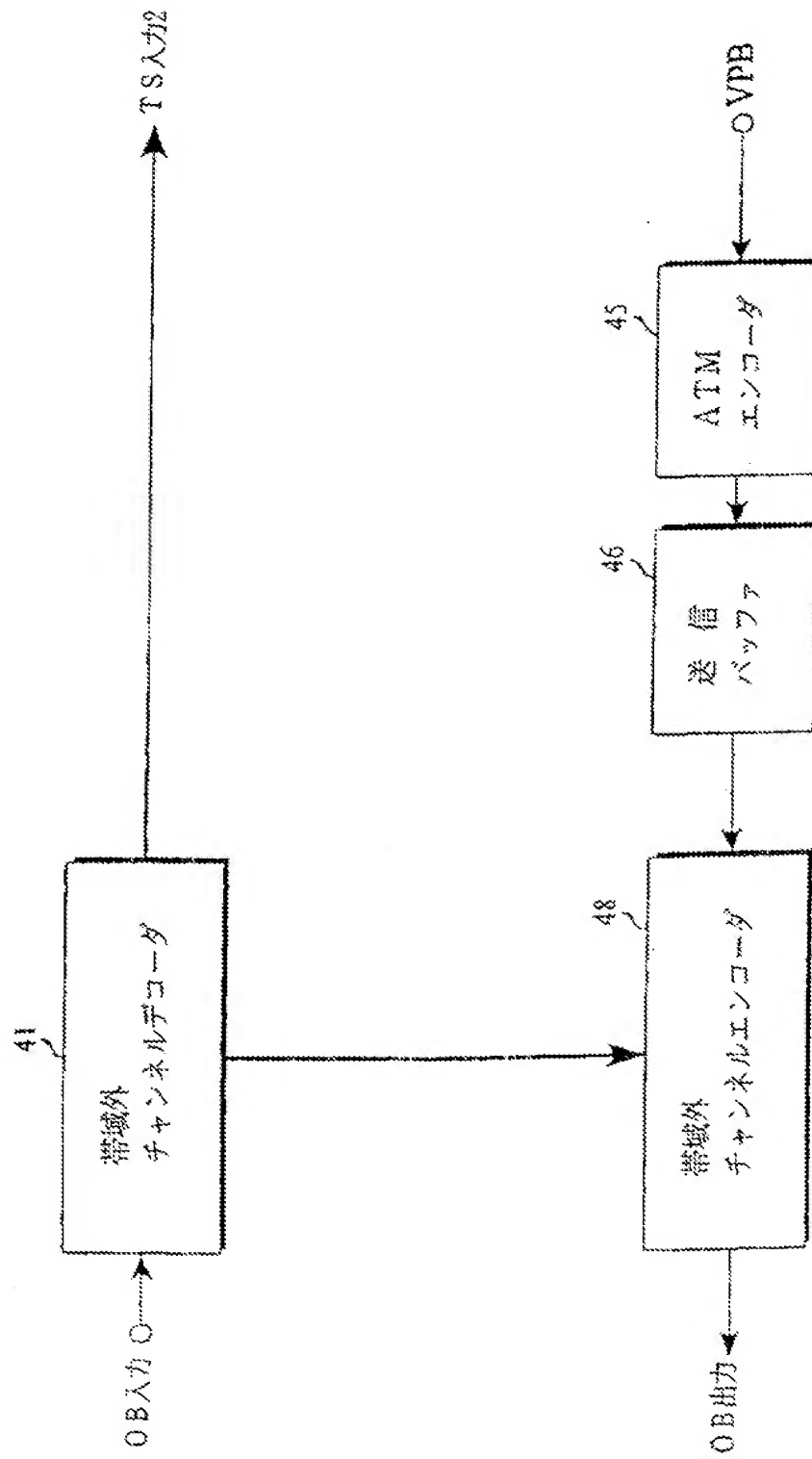
【図4】



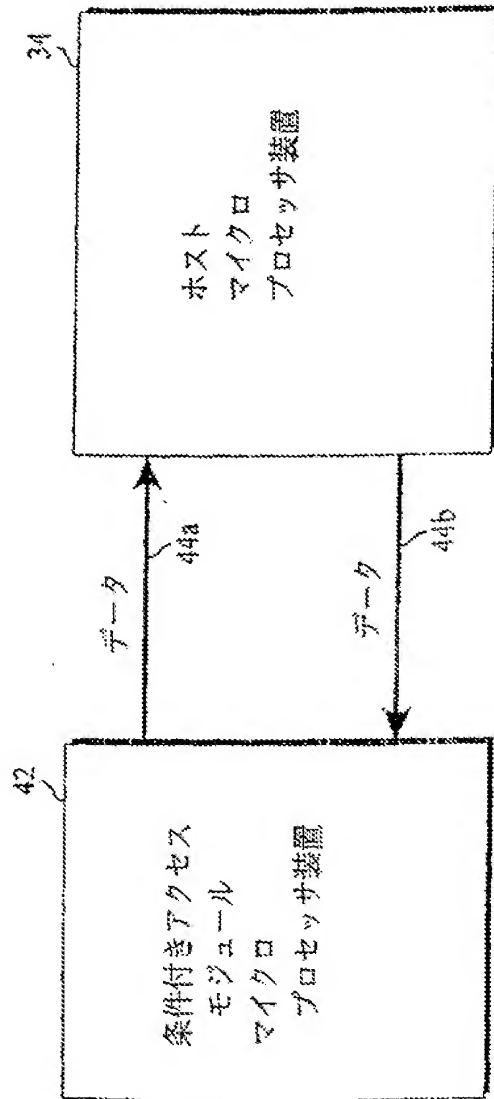
【図5】



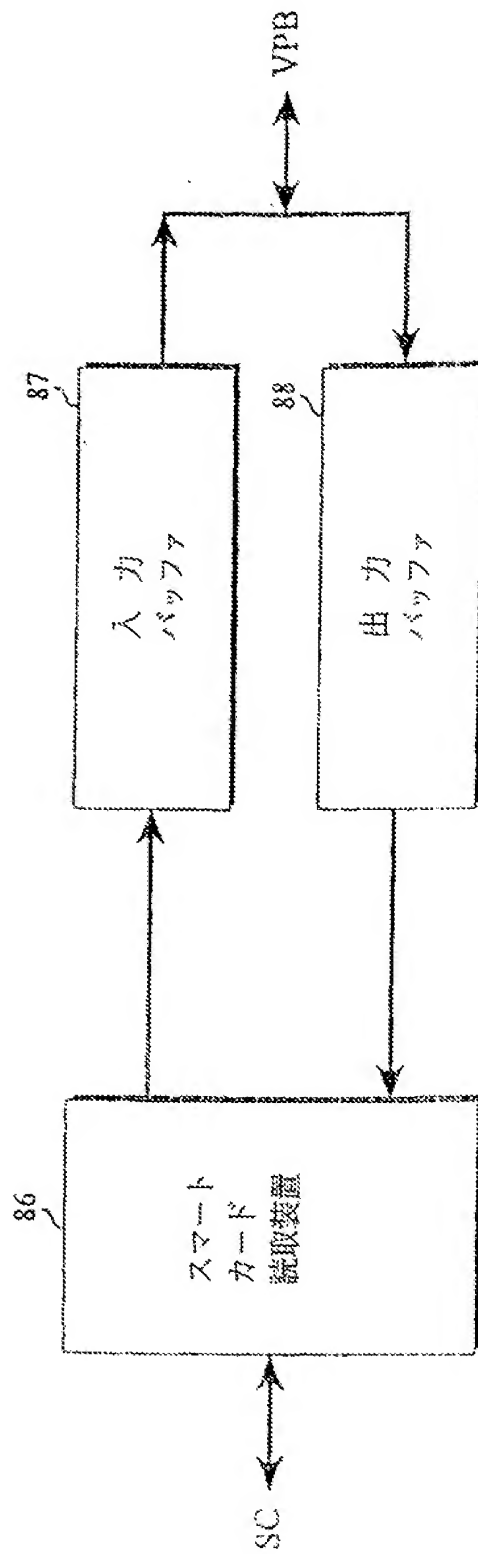
【図6】



【図7】

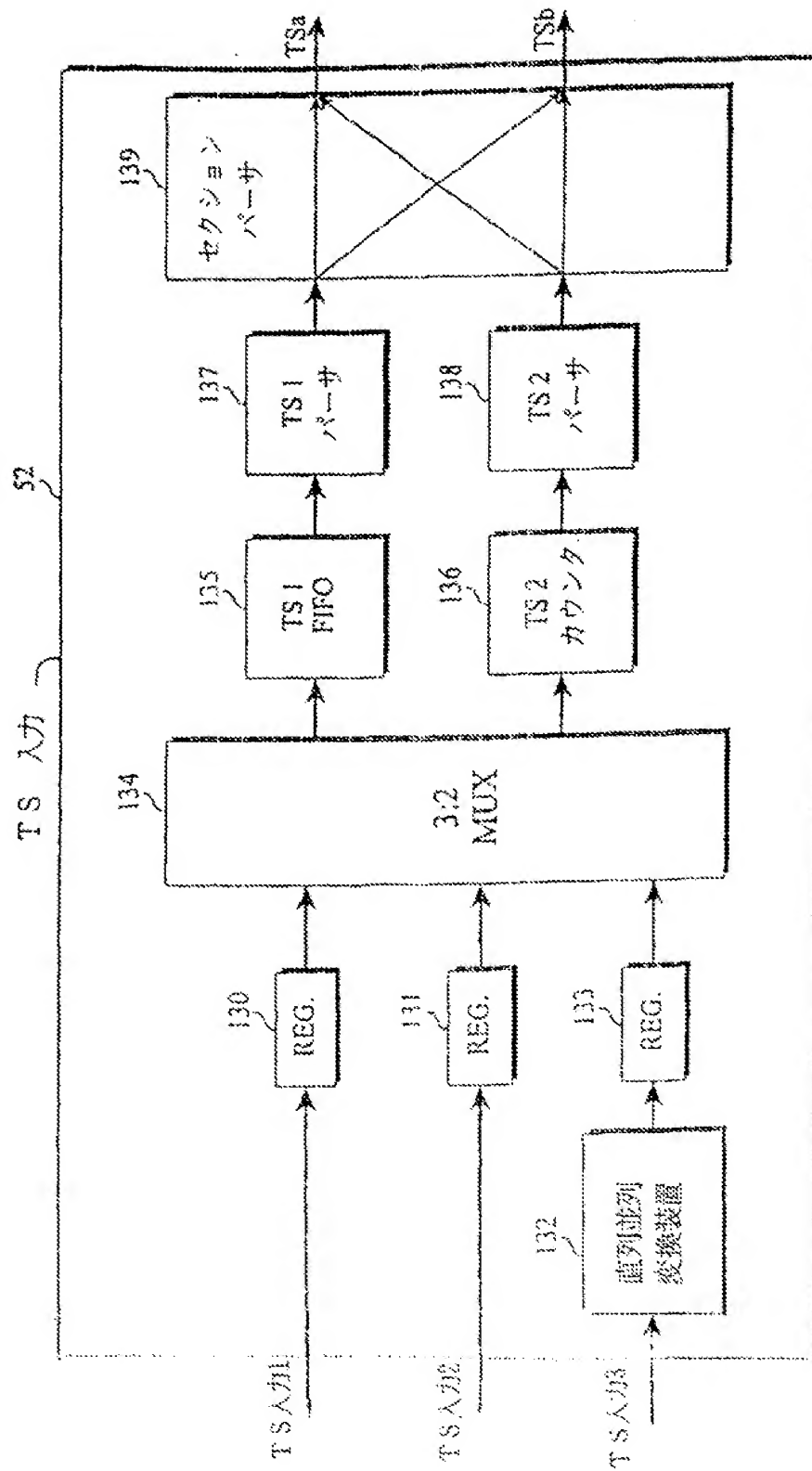


【図8】

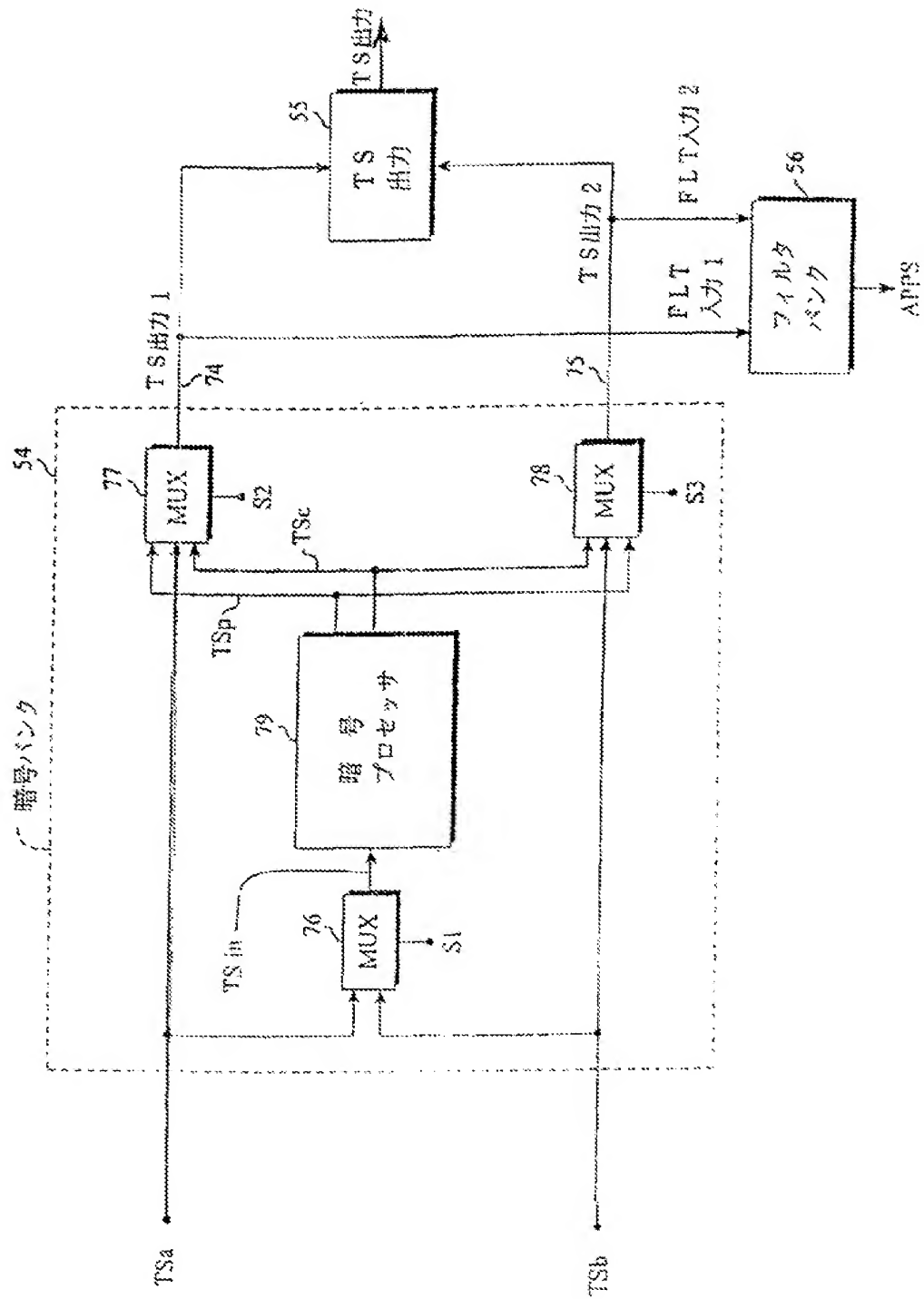




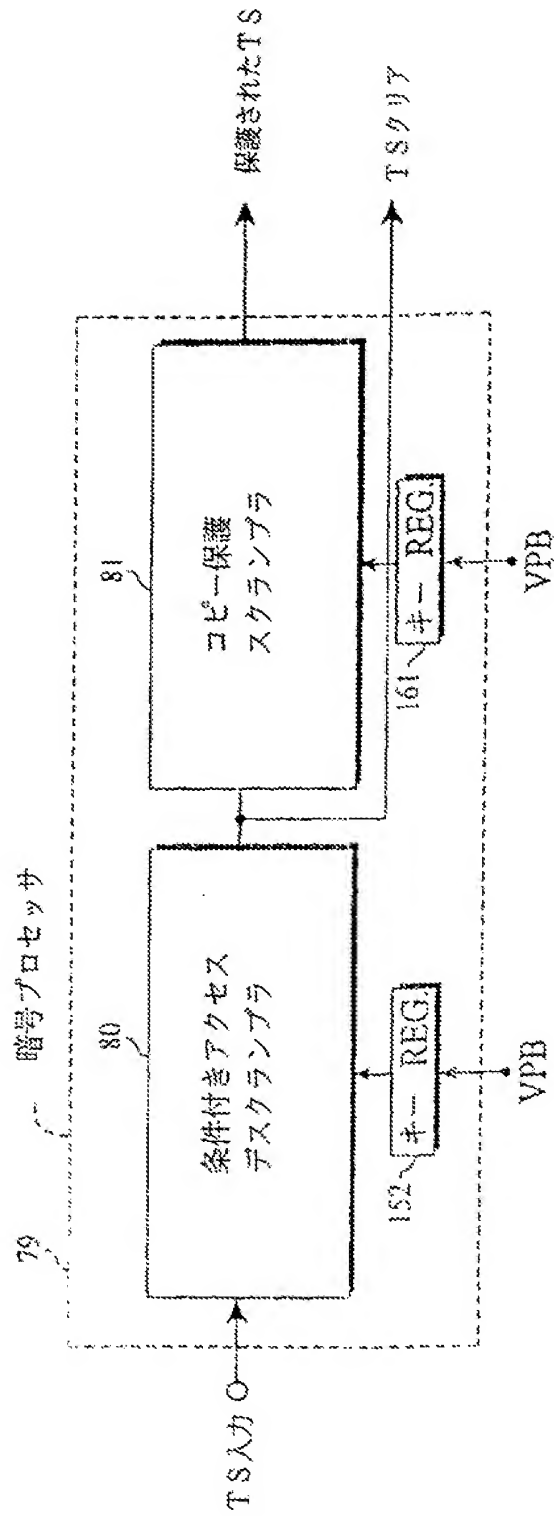
【図9】



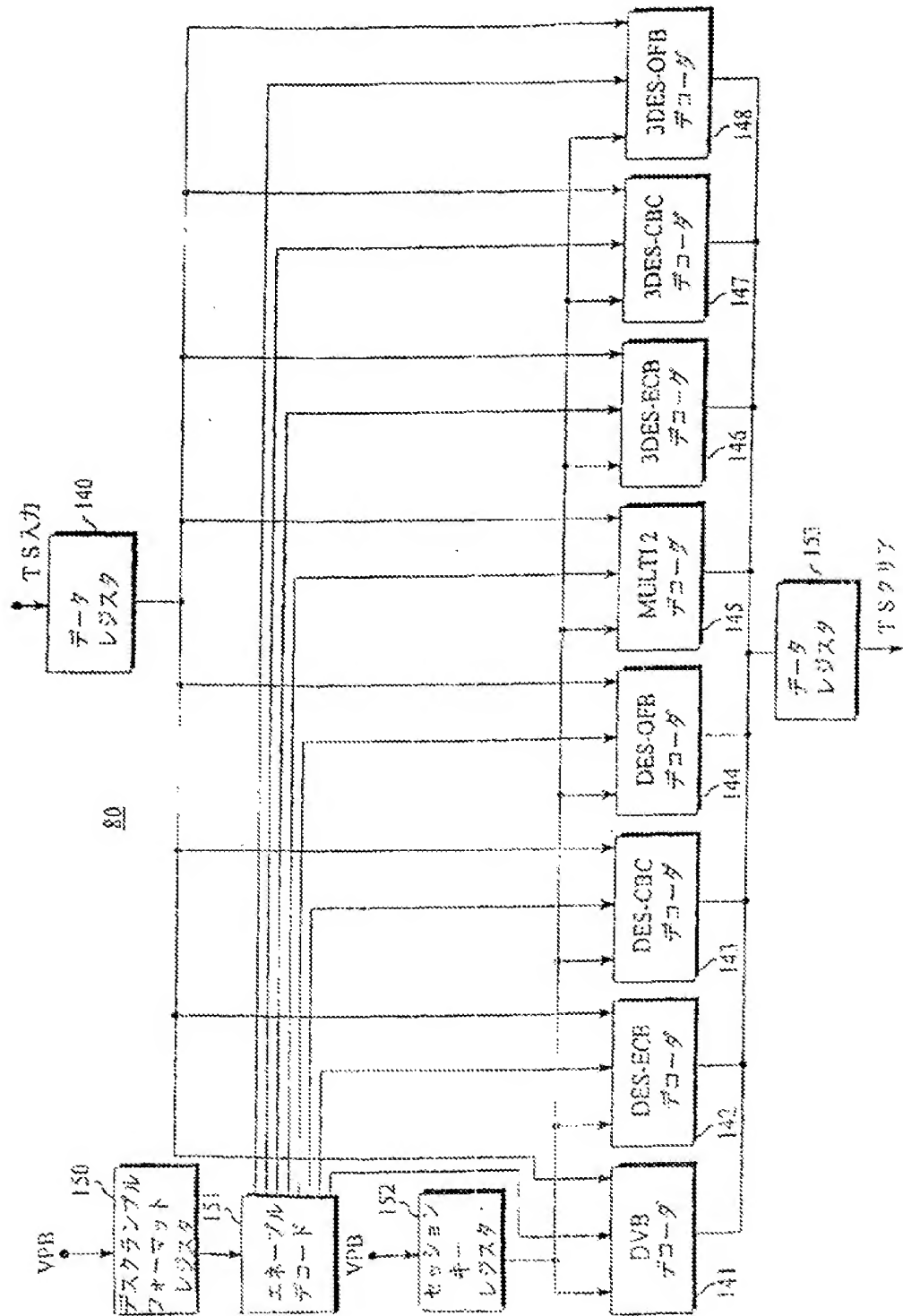
【図10】



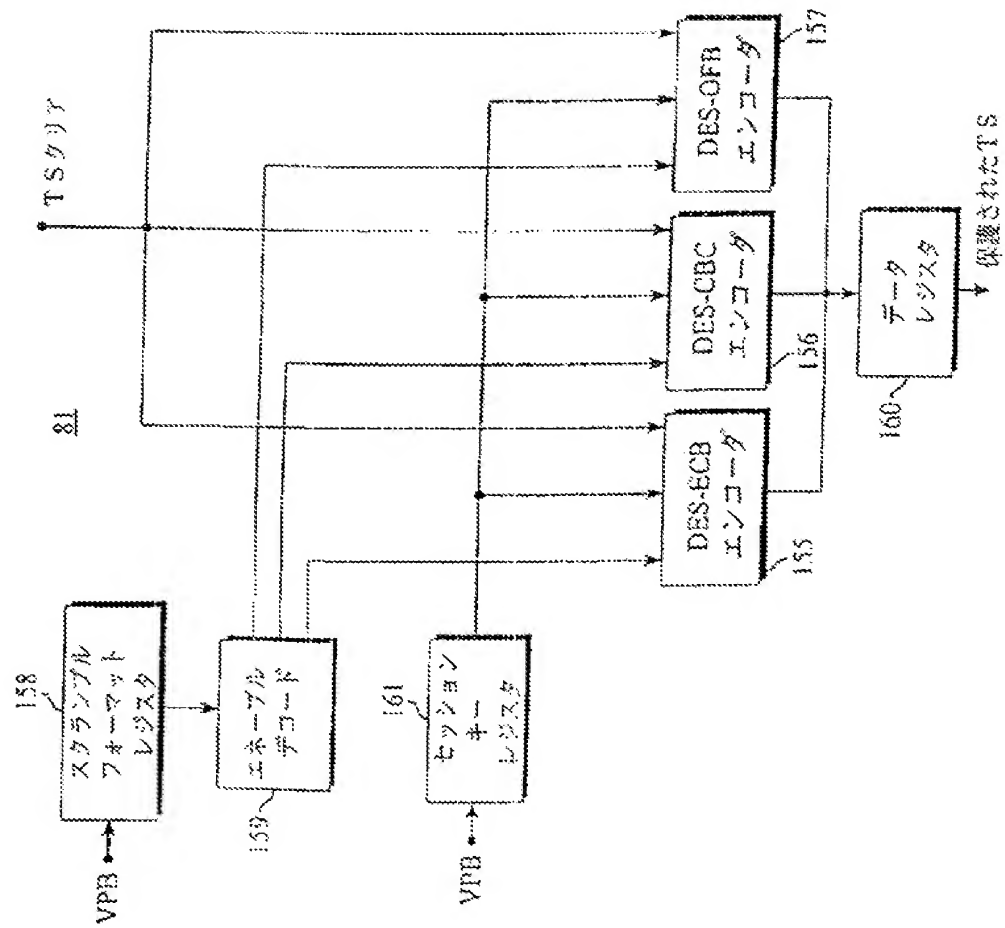
【図11】



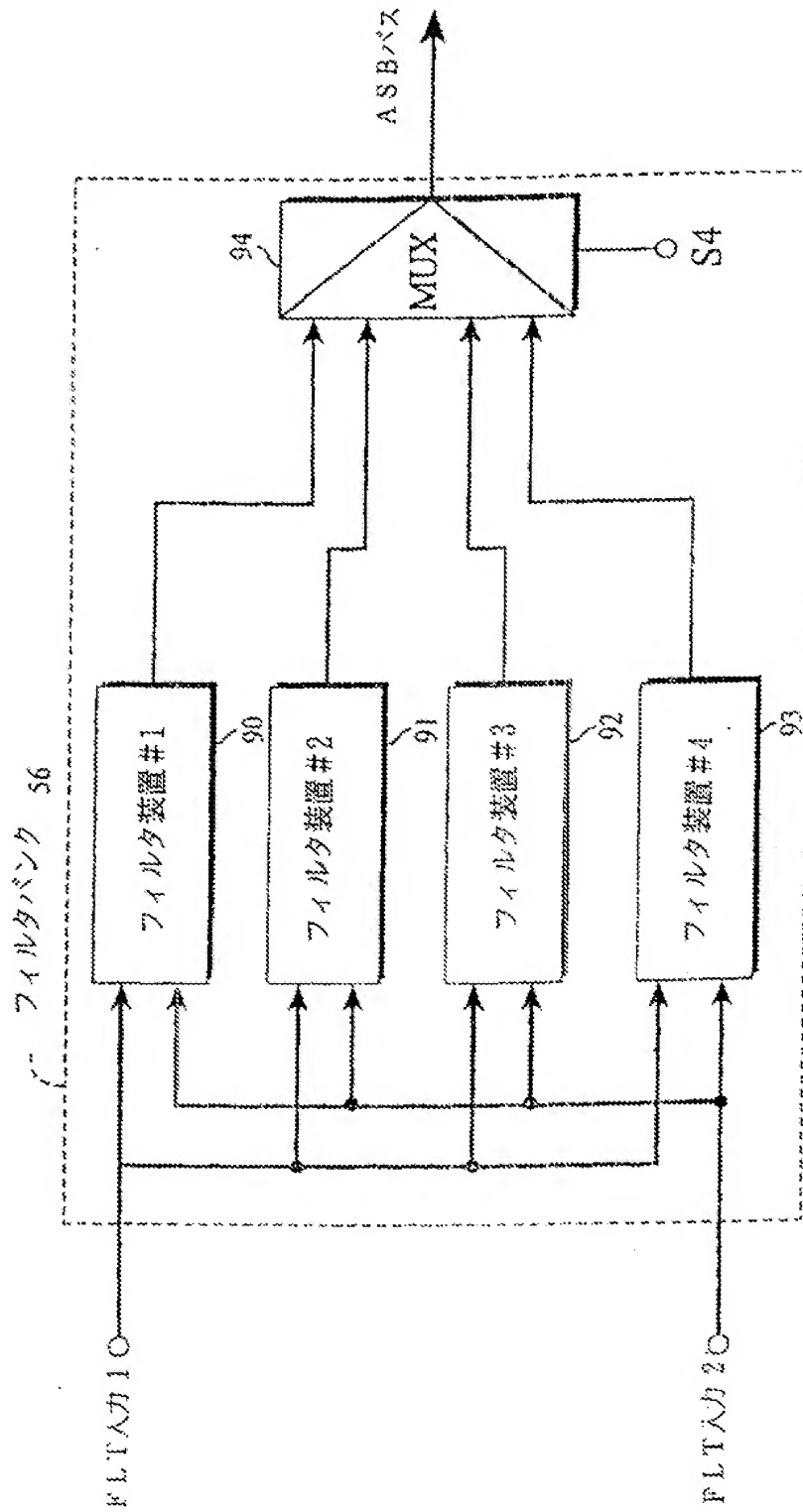
【図12】



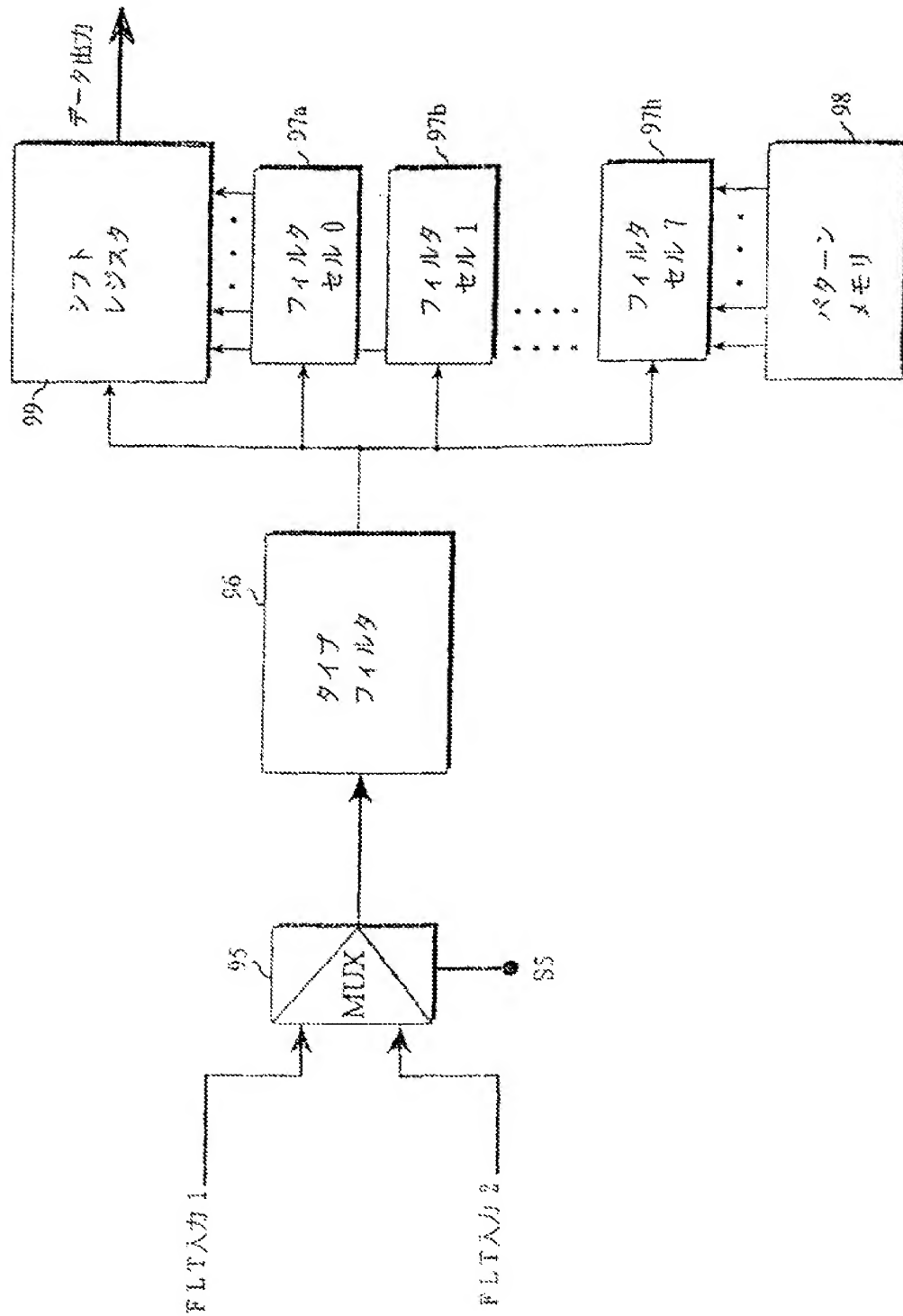
【図13】



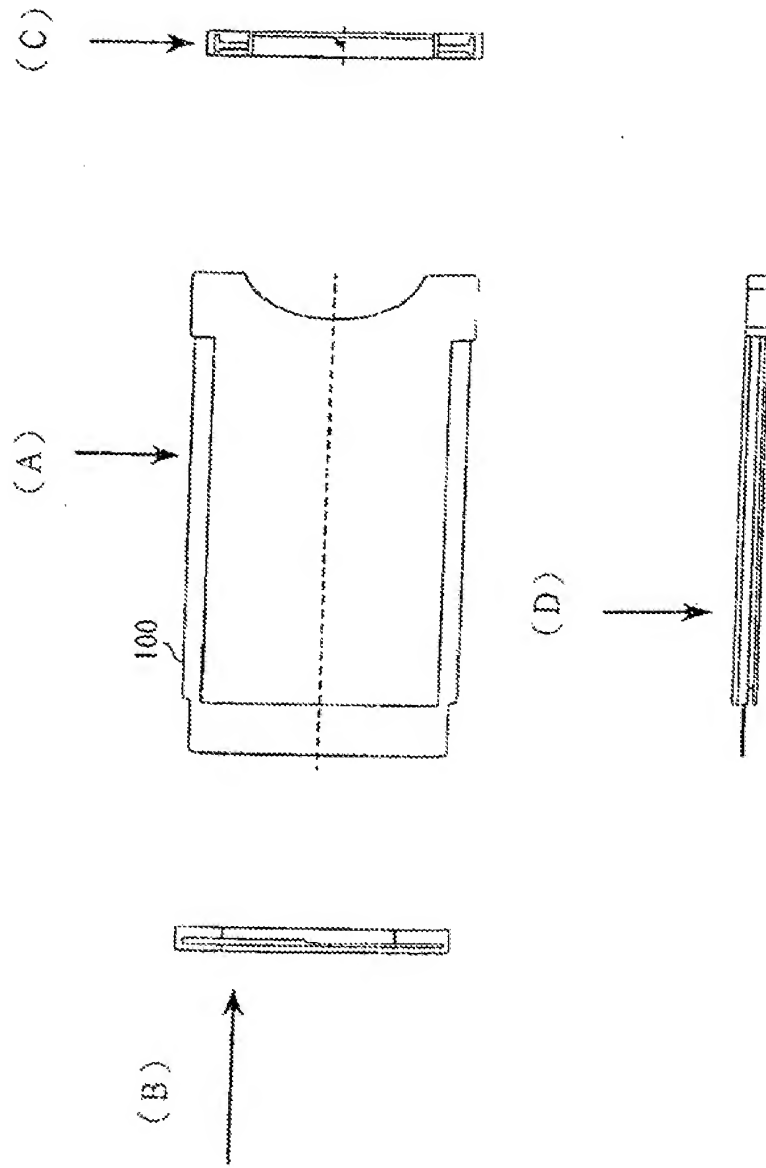
【図14】



【図15】

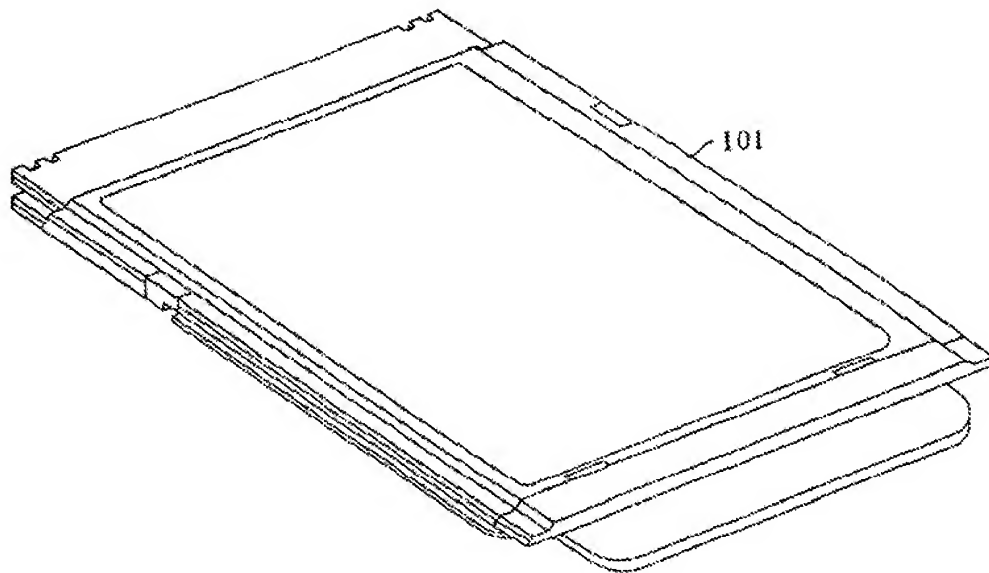


【図16】

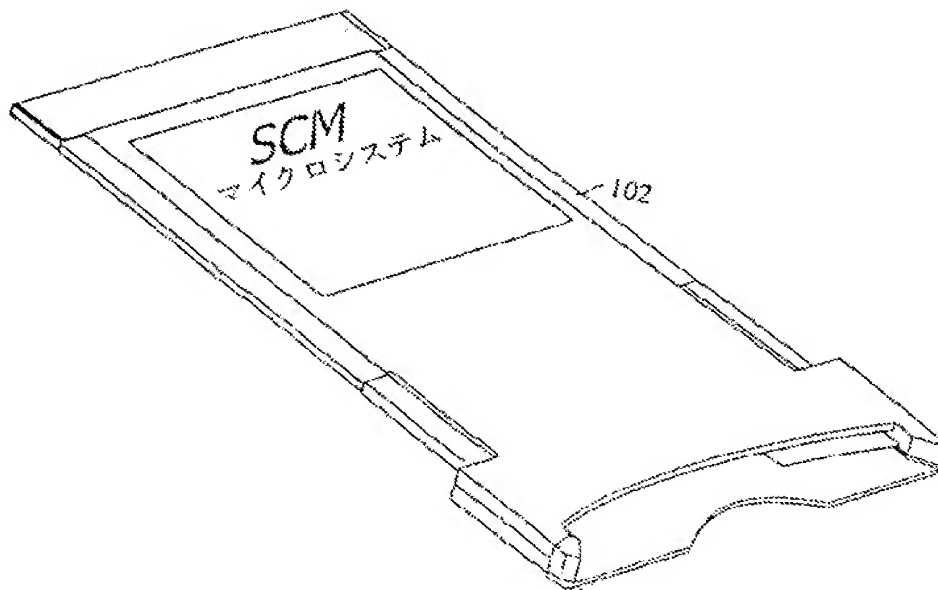




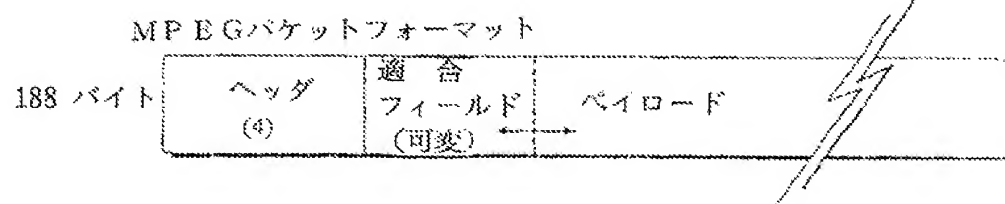
【図17】



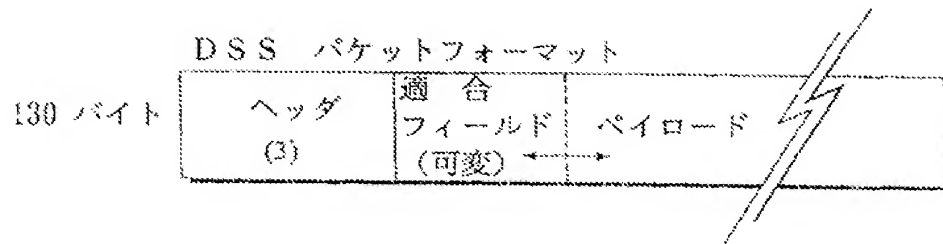
【図18】



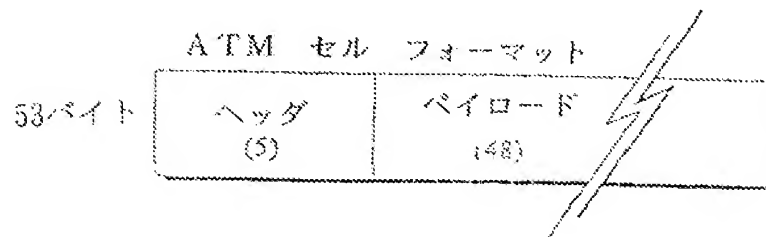
【図19】



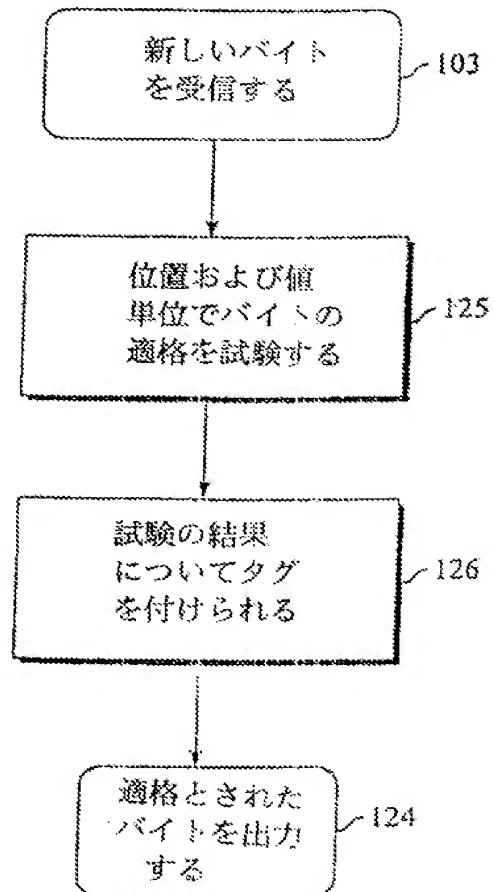
【図20】



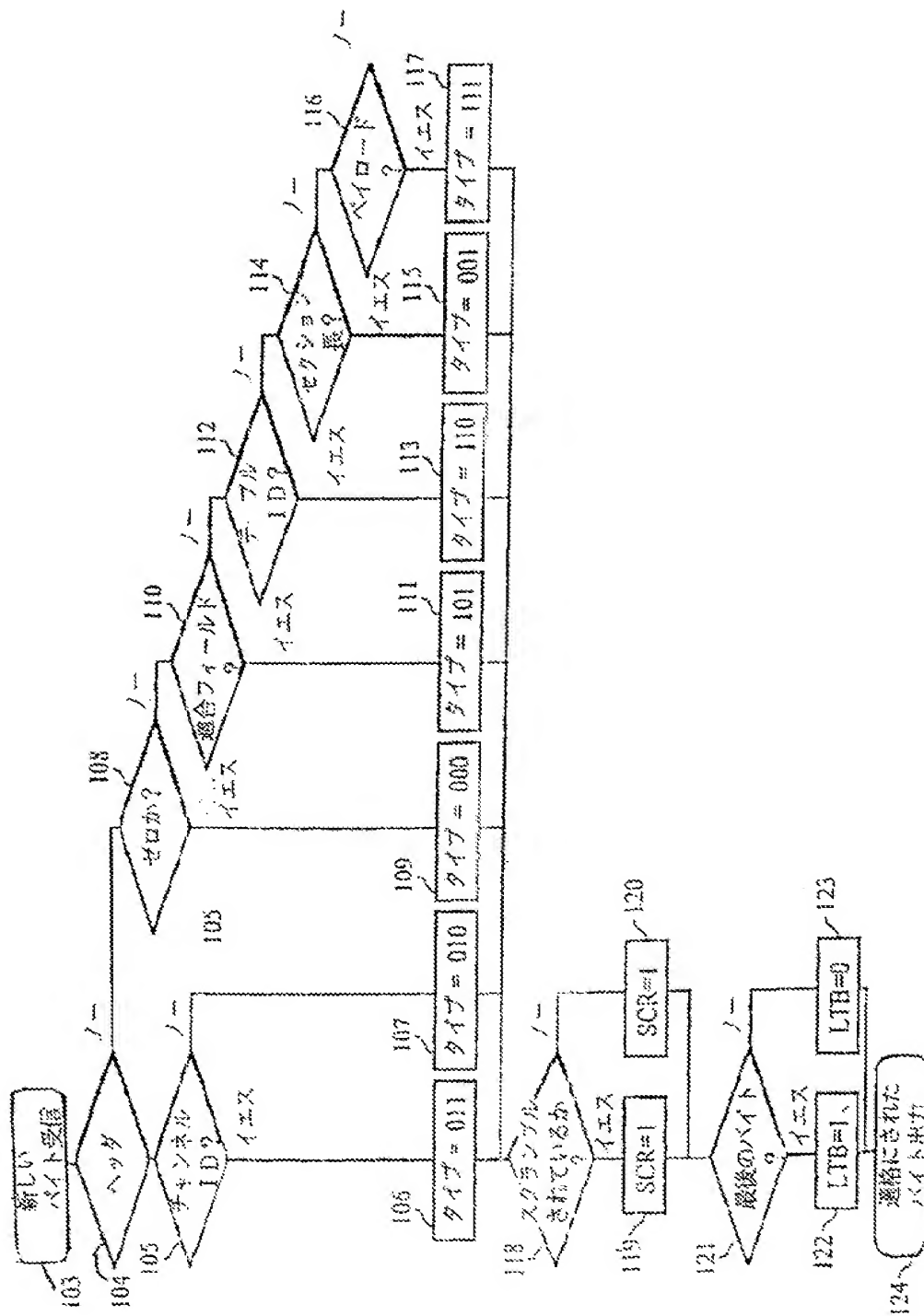
【図21】



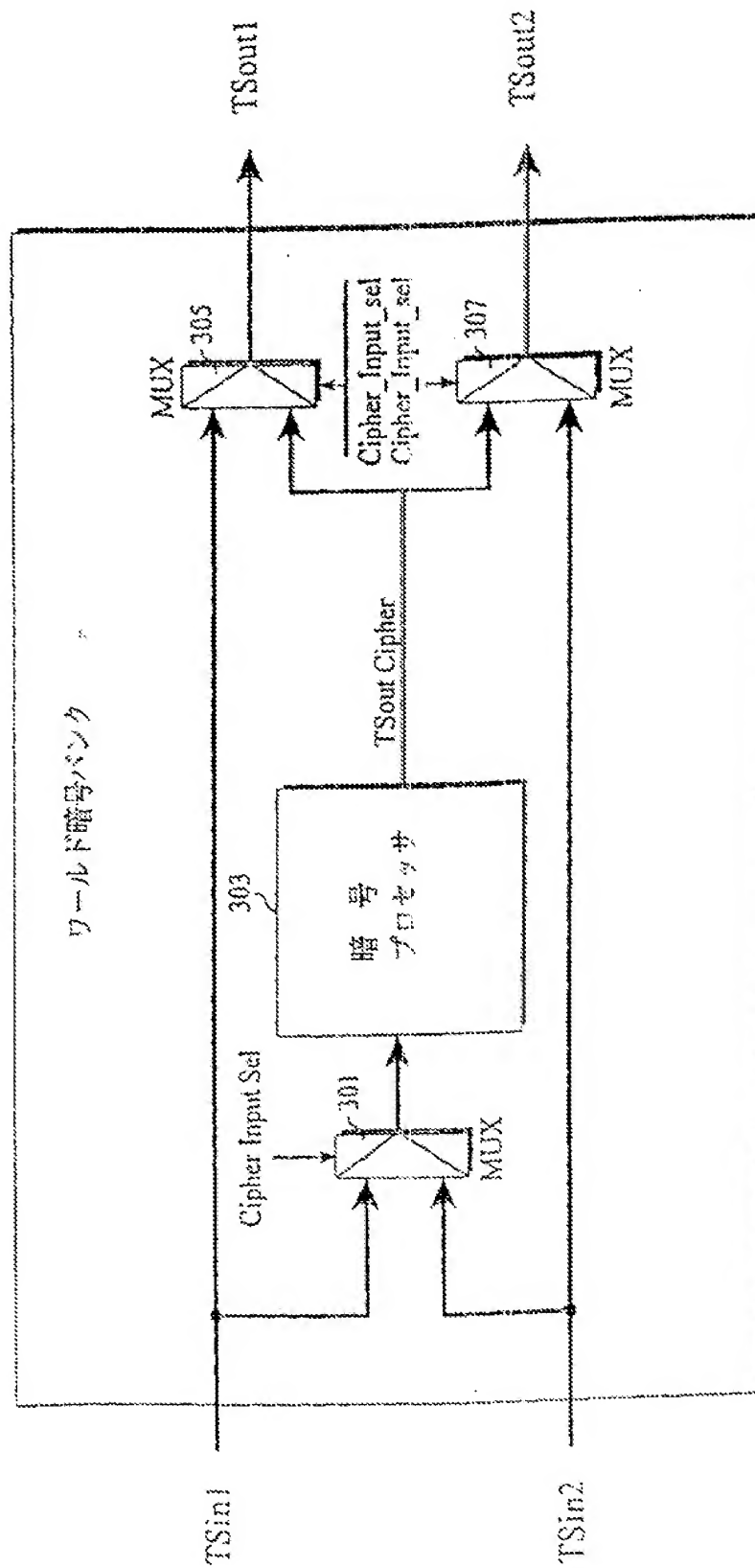
【図22】



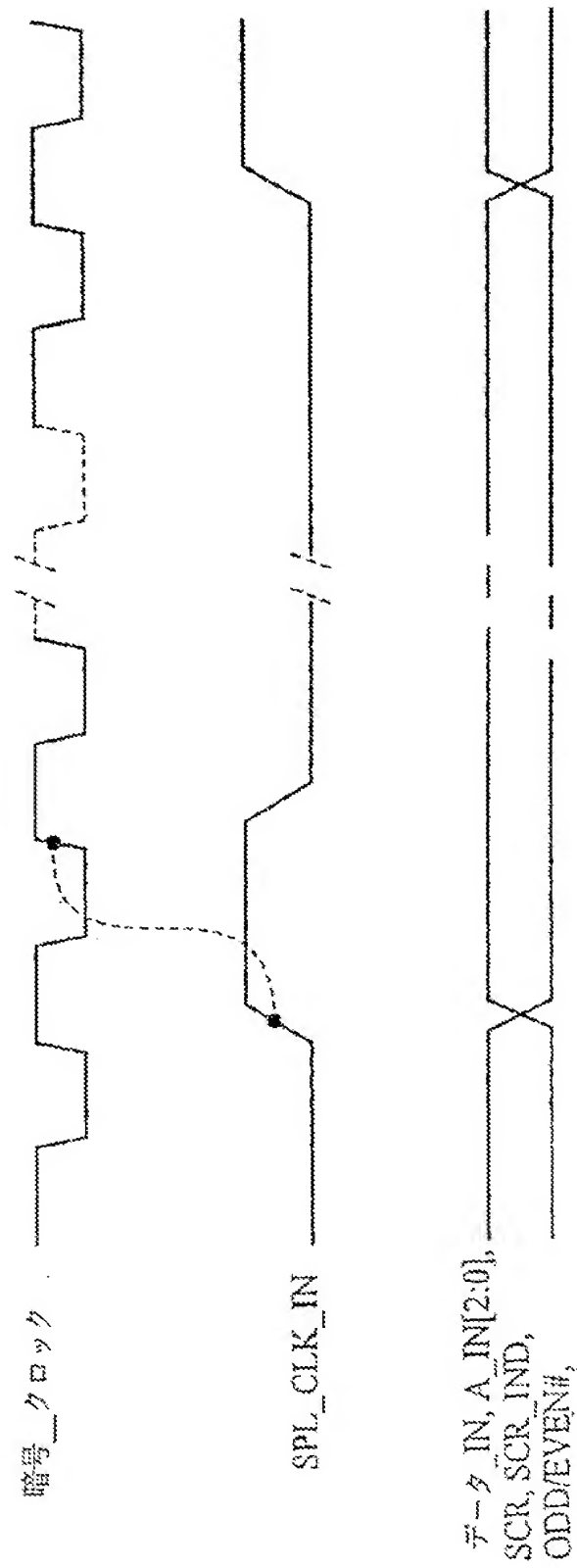
【図23】



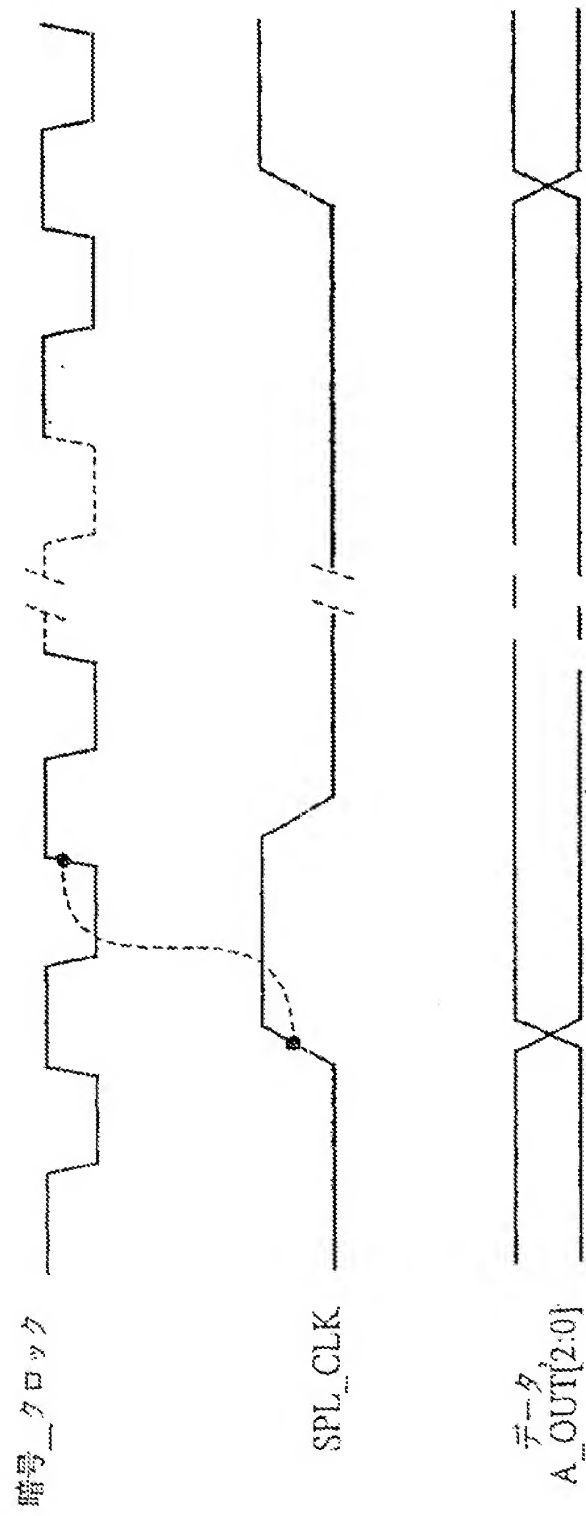
【図24】



【図25】



【図26】



**【手続補正書】**

**【提出日】** 平成14年6月27日 (2002. 6. 27)

**【手続補正1】**

**【補正対象書類名】** 明細書

**【補正対象項目名】** 特許請求の範囲

**【補正方法】** 変更

**【補正の内容】**

**【特許請求の範囲】**

**【請求項1】** 複数の転送フォーマットのうちの選択された1つであり、複数の暗号フォーマットのうちの選択された1つである信号をネットワークから受信するための受信回路と、

受信された信号を検査し、それに関する転送フォーマットと無関係の情報信号を生成するための回路と、

受信された信号のネットワーク暗号化部分をデスクランブルし、このような部分をエンドユーザに必要なコピー保護暗号化フォーマットにしたがって再スクランブルするためのトランススクランブル回路と、

受信された信号から補助情報を抽出するための濾波回路と、

トランススクランブル回路を制御するために、転送フォーマットと無関係の情報信号と、抽出された補助情報とに応答する制御回路とを具備している適応受信システム。

**【請求項2】** 複数の転送フォーマットのうちの選択された1つであり複数の暗号フォーマットのうちの選択された1つである信号をネットワークから受信し、

受信された信号を検査し、それに関する転送フォーマットと無関係の情報信号を生成し、

受信された信号のネットワーク暗号化部分をデスクランブルし、このような部分をエンドユーザに必要なコピー保護暗号化フォーマットにしたがって再スクランブルし、

受信された信号から補助情報を抽出し、

デスクランブルおよび再スクランブル動作を制御するために、転送フォーマットと無関係の情報信号と、抽出された補助情報とを使用する適応信号受信方法。

【請求項3】 複数の異なるデジタル送信フォーマットの1つでデジタルデータ流を受信する入力信号チャンネルと、

入来するデータ流を送信フォーマットと無関係の信号のセットへ変換する回路と、

送信フォーマットを変換するディスプレイ機構とを具備しているシステム。

【請求項4】 回路は入来するデータバイトの修飾機構と、各データバイトヘタグを割当てるタグ付け機構とを含み、受信システムはタグ付けされたデータバイトに応答する回路を含んでいる請求項3記載のシステム。

【請求項5】 修飾機構はパーサ機構を具備している請求項4記載のシステム。

【請求項6】 それぞれ複数の異なるフォーマットの1つで送信される少なくとも2つのデータ流を受信する少なくとも2つの入力チャンネルと、

それぞれの入来するデータ流をフォーマットに無関係の信号のセットへ変換する回路と、

フォーマットに無関係の信号をイメージへ変換する機構と、

フォーマットに無関係のメッセージ信号を感知可能なメッセージに変換するメッセージ処理機構とを具備している請求項3記載のシステム。

【請求項7】 回路は、

第1の修飾機構と、

第1のタグ付け機構と、

第1の信号処理回路と、

第2の修飾機構と、

第2のタグ付け機構と、

メッセージ信号をメッセージ処理機構へ供給するためにタグ付けされたメッセージ信号バイトに応答する第2の信号処理回路とを具備している請求項6記載のシステム。

【請求項8】 それぞれの修飾機構はパーサ機構を具備している請求項7記



載のシステム。

【請求項9】 データ装置でデータを受信し、  
データの暗号化状態を決定し、  
暗号化されていないデータの場合には、クリア出力を提供し、  
暗号化されたデータの場合には、受信されたデータ装置のユニットサイズを決定し、決定されたユニットサイズにしたがって暗号解読機能を行い、それによって暗号解読されたデータを与えるステップを含んでいる方法。

【請求項10】 所望のスクランブルフォーマットを選択し、  
セッションキーを選択し、  
選択されたメモリ中に選択されたセッションキーをロードする請求項9記載の方法。

【請求項11】 スクランブルフォーマットを選択するステップを含んでいる請求項9記載の方法。

【請求項12】 放送信号の処理を含んでいる請求項9記載の方法。

【請求項13】 バースト信号の処理を含んでいる請求項9記載の方法。

【請求項14】 異なるデータ暗号化フォーマットにしたがってスクランブルする複数のエンコーダ機構と、クリア情報をスクランブルするために特定のエンコーダ機構を選択するエンコーダ選択機構とを含んでいる請求項1乃至13のいずれか1項記載のシステム。

【請求項15】 受信されたデータバイトを修飾し、  
修飾されたデータバイトがスクランブルされているか否かおよびこれがコピー保護されるべきか否かを示すために受信された各データバイトにタグを取付けるステップを含んでいる複数の信号フォーマットを処理する方法。

【請求項16】 選択された条件付きアクセスモジュールまたはカードと選択されたモジュールとを対にし、  
コピー保護機構を選択し、  
スクランブルセッションキーを決定するステップを含んでいる請求項15記載の方法。

【請求項17】 記憶される前に私有暗号キーにしたがって信号をスクラン

ブルし、

再生されるときこの同一の私有暗号キーにしたがって記録された信号をデスクランブルするステップを含んでいる請求項15または16記載の方法。

【請求項18】 保護される信号を受信し、

受信された信号を局部的に生成される暗号キーにしたがってスクランブルし、スクランブルされた信号を信号記憶媒体に記録し、

記憶された信号を再生し、

再生された信号を局部的に発生された暗号キーにしたがってデスクランブルし、

、

デスクランブルされた信号をエンドユーザシステムに供給するステップを含んでいる請求項17記載の方法。

【請求項19】 複数のフォーマットのうちの1つを有しスクランブルを受ける制御およびコンテンツ情報を処理する方法において、

制御およびコンテンツ情報を受信し、修飾し、修飾状態にしたがってタグ付けし、

デスクランブル動作を決定するために修飾タグを使用し、

制御情報をコンテンツ情報から分離するステップを含んでいる方法。

【請求項20】 少なくとも1つの予め定められたセキュリティ層にしたがった1以上の信号送信ソースと通信するように構成されている複数の受信機と、

少なくとも1つのセキュリティ層を除去するように構成されている機構とを具備しているシステム。

【請求項21】 前記機構は条件付きアクセスモジュールである請求項20記載のシステム。

【請求項22】 それぞれ複数の異なるフォーマットの1つで送信される少なくとも2つのデータ流を受信する少なくとも2つの入力チャネルと、

それぞれの入来するデータ流をフォーマットに無関係の信号のセットへ変換する回路と、

フォーマットに無関係の信号をイメージへ変換する機構と、

フォーマットに無関係のメッセージ信号を感知可能なメッセージに変換するメ

ッセージ処理機構とを具備しているシステム。

【請求項23】 回路は、

第1の修飾機構と、

第1のタグ付け機構と、

第1の信号処理回路と、

第2の修飾機構と、

第2のタグ付け機構と、

メッセージ信号をメッセージ処理機構へ供給するためにタグ付けされたメッセージ信号バイトに応答する第2の信号処理回路とを具備している請求項22記載のシステム。

【請求項24】 それぞれの修飾機構はパーサ機構を具備している請求項23記載のシステム。

【請求項25】 第1の試験機構と、

タグを示すヘッダバイトを割当てるために第1の試験機構に結合されている第1のタグ付け機構と、

入来する各データバイトを検査してデータがスクランブルされているか否かを決定する第2の試験機構と、

スクランブル状態タグビットを各データバイトへ割当て、データがスクランブルされているならばこのようなビット2進値の一方を与え、データがスクランブルされていないならば2進値の他方を与えるように第2の試験機構に結合されている第2のタグ付け機構と、

使用可能なデジタル情報を生成するために、各データバイトおよびその割当てられたタグビットをデータ処理機構へ転送する信号転送回路とを具備している機構。

【請求項26】 データをスクランブルし、

選択されたホストと選択されたモジュールとを対にし、

所望のデスクランブルフォーマットを選択し、

セッションキーを選択するステップを含んでいる方法。

【請求項27】 データをデスクランブルし、

選択されたホストと選択されたモジュールとを対にし、  
所望のデスクランブルフォーマットを選択し、  
セッションキーを選択するステップを含んでいる請求項26記載の方法。

【請求項28】 以下の暗号化フォーマット、即ちDVB、DES-ECB、DES-CBC、DES-OFB、MULTI2、3DES-ECB、3DES-CBC、3DES-OFBの1つをデスクランブルするために複数のデコーダを有するデスクランブラを使用し、DVBはデジタルビデオ放送を意味し、DESはデータ暗号化標準方式を意味し、ECBは電子コードブックを意味し、CBCはチェンブロック暗号を意味し、OFBは出力フィードバックブロックを意味している請求項27記載の方法。

【請求項29】 異なるフォーマットにしたがってスクランブルされたデジタルデータ信号を受信するための入力回路と、  
受信された信号の暗号化フォーマットを識別する機構と、  
受信されたデータ信号をデスクランブルするデスクランブル機構と、  
デスクランブルされたデータ信号を再スクランブルするスクランブル機構とを具備しているシステム。

【請求項30】 デジタルテレビジョン受信システムを含んでいる請求項29記載のシステム。

【請求項31】 受信されたデータ信号は第1のデータ暗号化フォーマットにしたがってスクランブルされ、第2のデータ暗号化フォーマットにしたがって再スクランブルされる請求項29記載のシステム。

【請求項32】 第1のデータ暗号化フォーマットはDVB、DES-ECB、DES-CBC、DES-OFB、MULTI2、3DES-ECB、3DES-CBC、3DES-OFBから選択された1つのフォーマットであり、DVBはデジタルビデオ放送を意味し、DESはデータ暗号化標準方式を意味し、ECBは電子コードブックを意味し、CBCはチェンブロック暗号を意味し、OFBは出力フィードバックブロックを意味し、第2のデータ暗号化フォーマットはDESフォーマットである請求項31記載のシステム。

【請求項33】 スクランブル機構は、受信された信号の暗号化フォーマット

トとは異なるスクランブルされたデータ信号を生成する請求項32記載のシステム。

【請求項34】 受信されたデータ信号は、第1の複数の異なるデータ暗号化フォーマットのうちの特定の1つのフォーマットにしたがってスクランブルされ、第2の複数の異なるデータ暗号化フォーマットのうち特定の1つのフォーマットにしたがってスクランブルされるスクランブルデータ信号を生成する請求項32記載のシステム。

【請求項35】 受信されたデータ信号のスクランブルシーケンスはスクランブルキーによって制御される請求項32記載のシステム。

【請求項36】 デスクランブル機構はデータ信号をデスクランブルする複数のデコーダ機構とデコーダ選択機構とを具備している請求項32記載のシステム。

【請求項37】 異なるデータ暗号化フォーマットにしたがってスクランブルする複数のエンコーダ機構と、クリア情報をスクランブルするために特定のエンコーダ機構を選択するエンコーダ選択機構とを含んでいる請求項32記載のシステム。

【請求項38】 多数フォーマットの転送ストリームを受信する回路と、パケットまたはセル内の位置にしたがってデータバイトを識別する機構と、パケットまたはセル内の値にしたがってデータバイトを識別し、一致が検出されたとき一致指示信号を生成する機構と、一致指示信号に応答するデータ抽出機構とを具備している機構。

【請求項39】 保護されるべき信号を受信し、受信された信号を局所的に生成される暗号キーにしたがってスクランブルし、スクランブルされた信号を信号記憶媒体に記録し、記憶された信号を再生し、再生された信号を局所的に発生された暗号キーにしたがってデスクランブルし、  
、  
デスクランブルされた信号をエンドユーザシステムに供給するステップを含んでいる方法。

【請求項40】 受信されスクランブルされた信号のクリアコピーバージョンを生成するために、その信号をデスクランブルするためにその信号に応答するデスクランブラ機構と、

クリアコピー信号を私有暗号キーにしたがってスクランブルするためにその信号に応答するスクランブラ機構と、

私的にスクランブルされた信号の私的記憶コピーを生成するためにその信号を信号記憶媒体へ供給する回路を具備しているシステム。

【請求項41】 信号記憶媒体に記録された私的にスクランブルされた信号を再生し、このような私的にスクランブルされた信号は私的暗号キーにしたがってスクランブルされているプレイバック機構と、

その信号のクリアコピーバージョンを生成するために、私的暗号キーにしたがってその信号をデスクランブルするデスクランブラ機構と、

クリアコピー信号を条件付きアクセスシステムにより使用されるコピー保護暗号キーにしたがってスクランブルするためにその信号に応答するスクランブラ機構と、

コピー保護されたスクランブルされた信号をエンドユーザシステムへ供給する回路とを具備している請求項40記載のシステム。

## 【国際調査報告】

## INTERNATIONAL SEARCH REPORT

International Application No.  
PC, EP 00/11463A. CLASSIFICATION OF SUBJECT MATTER  
IPC 7 H04N5/00 H04N7/167

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication, where appropriate, of the relevant passages                                                                                                                                           | Relevant to claim no. |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| P, A       | WO 00 27114 A (GEN INSTRUMENT CORP<br>; KASSMAN TODD (US); PETERKA PETR (US);<br>MANGALO) 11 May 2000 (2000-05-11)<br>abstract<br>page 2, line 29 - page 7, line 2<br>page 8, line 2 - page 12, line 24<br>---               | 1, 2,<br>160-162      |
| A          | BUNGUM O W: "TRANSMULTIPLEXING,<br>TRANSCONTROL AND TRANSSCRAMBLING OF<br>MPEG-2/DVB SIGNAL"<br>INTERNATIONAL BROADCASTING CONVENTION,<br>12 September 1996 (1996-09-12),<br>XP002040478<br>the whole document<br>---<br>-/- | 1, 2,<br>160-162      |

☒ Further documents are listed in the continuation of box C.☒ Patent family members are listed in annex.

## \* Special categories of cited documents:

\*A\* document defining the general state of the art which is not considered to be of particular relevance

\*E\* earlier document but published on or after the international filing date

\*L\* document which may throw doubts on priority claims or which is cited to establish the publication date of another claim or other special reason (as specified)

\*O\* document referring to an oral disclosure, use, exhibition or other means

\*P\* document published prior to the international filing date but later than the priority date claimed

\*T\* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

\*X\* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

\*Y\* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is considered with one or more other such documents, such combination being obvious to a person skilled in the art.

\*S\* document member of the same patent family

Date of the actual completion of the international search

6 April 2001

Date of mailing of the international search report

11.06.01

Name and mailing address of the ISA

European Patent Office, P.O. Box 1, 5118 Patentplan 2  
No. 1, 2200 HV Rijswijk  
Tel. (+31-70) 340-2040, 1x.31 551 551 ext. 1  
Fax: (+31-70) 340-9018

Authorized officer

Ibruegger, J

## INTERNATIONAL SEARCH REPORT

International Application No.  
PC., EP 99/11483

| C. (Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT |                                                                                                                                  |                       |
|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| Category *                                            | Citation of document, with indication, where appropriate, of the relevant passages                                               | Relevant to claim No. |
| A                                                     | US 5 835 493 A (JOHNSON BRIAN ET AL)<br>19 November 1998 (1998-11-10)<br>abstract<br>column 1, line 28 -column 8, line 10<br>--- | 1,2,<br>160-162       |
| A                                                     | US 5 912 972 A (BARTON JAMES M)<br>15 June 1999 (1999-06-15)<br>column 1, line 22 -column 4, line 38<br>---                      | 1,2,<br>160-162       |
| P,A                                                   | WO 00 54493 A (DIVA SYSTEMS CORP)<br>14 September 2000 (2000-09-14)<br>page 5, line 15 -page 12, line 20<br>---                  | 1,2,<br>160-162       |
| A                                                     | WO 97 18674 A (WYTEC INC)<br>22 May 1997 (1997-05-22)<br>page 5, line 2-14<br>page 12, line 18 -page 18, line 19<br>-----        | 1,2,<br>160-162       |



## INTERNATIONAL SEARCH REPORT

national application No.  
PCT/EP 00/11483

## Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:  
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos.:  
because they relate to parts of the international Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:
3. ☐ Claims Nos.:  
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

## Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1,2, 160-162

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest.
- ☐ No protest accompanied the payment of additional search fees.

## FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

## 1. Claims: 1,2,160-162

Adaptive receiving system for receiving signals in a plurality of transport formats and a plurality of encryption formats, generating transport format independent information, trans-scrambling encrypted portions of the received signals, extracting auxiliary information from the received signals and controlling the trans-scrambling in response to the transport format independent information and the extracted auxiliary information.

## 2. Claims: 3-7,43-47,72-79

Reception and qualification of data units, determination of the encryption state, providing a clear output, if the data are unencrypted and performing decryption, if the data are encrypted.

## 3. Claims: 8-18,39,80-100,130-134

Handling of a plurality of transport stream formats by a qualification mechanism and a tagging mechanism applying multibit tags to each received data byte.

## 4. Claims: 19-23,40,41,101-112

Reception of one or more signals of a selected transport format by a plurality of receivers and selection of a received signal by a security mechanism for removing at least a single security layer.

## 5. Claims: 24-27

Reception of one or more signals subject to at least a single predetermined security layer and removal of the at least single security layer.

## 6. Claims: 28-32

Selection of a transport stream format and security mechanism for selecting one or more transport streams.

## 7. Claims: 33-38

Reception of different digital transmission format data streams, conversion of the data streams into perceivable

## FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

information via a transmission format independent set of signals.

## 8. Claim : 42

First testing and tagging, second testing for determining whether data are scrambled and second tagging in response to second testing for assigning a scramble condition tag and transfer of signals for producing usable digital information.

## 9. Claims: 48-51,52-64

Scrambling/descrambling by pairing of a host with a selected module, selection of a scrambling format and a session key.

## 10. Claims: 65-69

Scrambler comprising a scramble format register and selection of an encoder by a control signal.

## 11. Claims: 70,71,126-128

Scrambling by channel change, selection of a descrambling mechanism, changing a session key and loading a new session key.

## 12. Claims: 113-123

Receiving signals scrambled according to different scrambling formats, descrambling and rescrumbling.

## 13. Claim : 124

Decryption of first type encrypted information and re-encrypting the information with a second type of encryption.

## 14. Claim : 125

Receiving of qualified information and if the received information is not scrambled passing the information without scrambling.

## 15. Claim : 129

Pairing of a conditional access module with a selected module, selecting a copy protect mechanism and determining a

## FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

scrambling session key.

## 16. Claims: 135,136

Detection of digital patterns within received digital signals and transfer of data bytes associated with the patterns to different end use locations.

## 17. Claim : 137

Filter for separating a plurality of digital data transport streams intended for different end uses, short and long term storage and multiplexing long and short term stored data in a time shared manner.

## 18. Claims: 138-157

Scrambling of data in conjunction with recording and descrambling in conjunction with playback.

## 19. Claim : 158

Multiformat signal system comprising a multitransport receiving system, a multiscrambling system and a multifiltering system.

## 20. Claim : 159

Use of a tag to determine a descrambling operation and separation of control from content information.

## INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No.

PC, JP 00/11483

| Patent document<br>cited in search report | Publication<br>date | Patent family<br>member(s) | Publication<br>date |
|-------------------------------------------|---------------------|----------------------------|---------------------|
| WO 0027114 A                              | 11-05-2000          | AU 1455100 A               | 22-05-2000          |
| US 5835493 A                              | 10-11-1998          | US 5002687 A               | 14-12-1999          |
| US 5912972 A                              | 15-05-1999          | US 5646997 A               | 08-07-1997          |
|                                           |                     | US 6115818 A               | 05-09-2000          |
|                                           |                     | US 6047374 A               | 04-04-2000          |
|                                           |                     | US 6101604 A               | 08-08-2000          |
|                                           |                     | US 6163842 A               | 19-12-2000          |
| WO 0054493 A                              | 14-09-2000          | US 6229895 B               | 08-05-2001          |
|                                           |                     | AU 3878900 A               | 28-09-2000          |
| WO 9718674 A                              | 22-05-1997          | US 5875396 A               | 23-02-1999          |
|                                           |                     | CA 2236088 A               | 22-05-1997          |
|                                           |                     | CN 1202295 A               | 16-12-1998          |
|                                           |                     | EP 0861559 A               | 02-09-1998          |
|                                           |                     | JP 2000500628 T            | 18-01-2000          |

---

フロントページの続き

(72)発明者 ジュヌボワ、クリストフ  
フランス国、エフー13600 ラ・シオタ、  
アブニュ・ドウ・ラ・ペ 47  
Fターム(参考) 5C025 BA01 BA14 BA25 CA02 DA01  
5C064 BA01 BC20 BC22 BC25 BD08  
BD09 CA01 CA14  
5J104 NA03 PA07